SolarWinds Orion NetFlow Traffic Analyzer

Evaluation Guide

Orion NetFlow Traffic Analyzer Evaluation Guide, Version 3.7, 08.10.2010

Acerca de SolarWinds (Vientos Solares)

SolarWinds, Inc. desarrolla y comercializa una amplia gama de gestión de red, monitoreo y herramientas de descubrimiento para satisfacer las diversas necesidades de gestión de la red de hoy en día y de profesionales de consultoría. Los productos SolarWinds siguen siendo los puntos de referencia por su calidad y rendimiento y han posicionado a la compañía como líder en gestión de redes y tecnología de descubrimiento. La base de clientes SolarWinds incluye más de 45 por ciento de las empresas Fortune 500 y los clientes de más de 90 países. Nuestro socio de negocios globales en red de distribuidores exceden los 100 distribuidores y revendedores. Contactando a SolarWinds…

Usted puede contactar SolarWinds de diversas maneras, incluyendo las siguientes:

Grupo	Información del contacto
Ventas	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Soporte técnico	www.solarwinds.com/support
Foros de usuarios	www.thwack.com

convenios

La documentación usa convenios consistentes en ayudarlo a identificar ítems en toda la librería impresa y online.

Convenio	Especificando
Negrita	Ítems de Windows, incluidos los botones y los campos.
cursiva	Libro y CD de títulos, nombres de variables, los nuevos términos
`Fuentes fijas`	Nombres de archivos y directorios, comandos y ejemplos de códigos, textos escritos por usted.
Entre paréntesis rectos, como en [valor]	Los parámetros opcionales de comandos.
Llaves, como en {valor}	Los parámetros requeridos de comandos.
Orden lógico como en valor*1*| valor2	Parámetros exclusivos de comandos en que solo una de las opciones se pueden especificar.

Librería de documentación de Orion NetFlow Traffic Analyzer

Los siguientes documentos se incluyen en la colección de Orion NetFlow Traffic Analyzer :

Documento	Propósito
Guía de administrador	Proporciona información detallada de la instalación, configuración, y la información conceptual.
Guía de evaluación	Proporciona una introducción a las características Orion NetFlow Traffic Analyzer e instrucciones para la instalación y configuración inicial.
Página de ayuda	Proporciona ayuda para todas las ventanas en la interfaz de usuario Orion NetFlow Traffic Analyzer.
Notas de la publicación	Proporciona información de última hora, los problemas conocidos, y las actualizaciones en: www.solarwinds.com.

Los siguientes documentos suplementan la biblioteca de Orion NetFlow Traffic Analyzer Documentation con información sobre Orion Network Performance Monitor (monitor de perfomance de trabajo en la red) :

Documento	Propósito
Guía de evaluación de monitor de rendimiento de redes de orion	Proporciona información detallada de instalación, configuración, y la información conceptual de Orion network performance monitor.
Orion Network Performance Monitor Evaluation Guide	Provides an introduction to Orion Network Performance Monitor features and instructions for installation and initial configuration.
Página de Ayuda	Proporciona ayuda para todas las ventanas en la interfaz de usuario Orion Network Performance Monitor
Notas de la publicación	Proporciona información de última hora, los problemas conocidos, y las actualizaciones. Las últimas notas de la versión se puede encontrar en: www.solarwinds.com.

Índice

Capítulo 1

Introducción a Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer (Orion NTA) proporciona una solucion escalable de monitoreo de red profesional, facil de usar y de cualquier tamaño NetFlow, sFlow-, J-Flow. O CBQoS permitido a la red.

Como las empresas y sus redes crecen, las necesidades de ancho de banda crecen exponencialmente. Todas las industrias modernas relacionadas invierten cantidades significativas de tiempo y dinero para asegurarse de que tienen suficiente ancho de banda disponible para las actividades críticas de negocio y sus aplicaciones. Cuando las necesidades de ancho de banda superan a la capacidad disponibles actualmente o cuando la demanda parece expandirse más allá de las capacidades de su red, entender el uso de ancho de banda ya no es un interés nuevo, pero se convierte en fundamental para decidir si es necesario invertir en más ancho de banda o si las pautas de uso más estrictas son suficientes para recuperar la pérdida de ancho de banda.

Con el advenimiento de los medios de transmisión de voz sobre IP (VoIP), tecnologías, juegos en línea y otras aplicaciones intensivas de banda ancha, usted, como ingeniero de redes, debe responder más que la simple pregunta de si la red está arriba o abajo.Usted debe responder por qué la red no se ajustan a las expectativas.

Si lo que necesita saber cómo y por quién el ancho de banda se está utilizando, Orion NetFlow Traffic Analyzer ofrece una respuesta sencilla e integrada. Usted puede rastrear y controlar el uso del ancho de banda de una aplicación en particular o el tipo de tráfico. Por ejemplo, si usted ve el uso excesivo de ancho de banda en una interfaz determinada, puede utilizar Orion NetFlow Traffic Analyzer para ver que la reunión de la compañía, que consiste en streaming de video, está consumiendo el 80% del ancho de banda disponible a través de un interruptor particular. A diferencia de muchos otros productos NetFlow análisis, los datos de red y NetFlow proporcionada por la solución de Orion NetFlow Traffic Analyzer no son puramente extrapolar los datos, sino que se basan en datos reales recogidos de la red por el producto Orion Network Performance Monitor (monitor de perfomance de redes Orion) que se encuentra en el corazón de Orion NetFlow Analyzer tráfico.

Fuera de la caja, Orion NetFlow Traffic Analyzer ofrece un amplio seguimiento y capacidades de gráficos, junto con las estadísticas testeadas a detalle, incluyendo las siguientes: Distribución de ancho de banda a través de tráfico

- Uso de los patrones en el tiempo
- Factores externos de identificación de trafico y de seguimiento

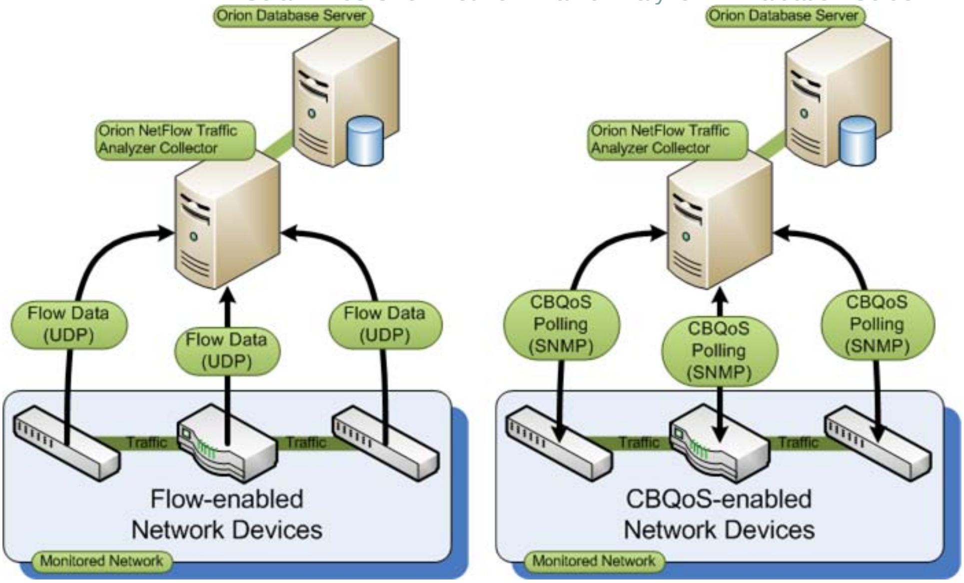
Estrecha integración con detalladas estadísticas de la interfaz de rendimiento. Estas capacidades de control, junto con el personalizable Orion Network Performance Monitor de la consola web y los motores de la presentación de informes, hacen que Orion NetFlow Traffic Analyzer sea su mejor opción para el control de su flujo de red habilitada.
.

Como trabaja Orion NetFlow Traffic Analyzer

Flujo y dispositivos CBQoS pueden proporcionar una gran cantidad de información sobre propiedad intelectual relacionados con el tráfico. Orion NTA recoge estos datos de tráfico, se correlaciona en un formato utilizable y, a continuación se presenta, con datos detallados de rendimiento de la red recogido por SolarWinds Orion Network Performance Monitor, como es fácil leer los gráficos e informes sobre el uso de ancho de banda de la red. Estos informes ayudan a controlar y la forma de uso de ancho de banda, las conversaciones entre los extremos de la pista interna y externa, analizar los patrones de tráfico, y el plan de necesidades de capacidad de ancho de banda.

El siguiente diagrama ofrece una visión general de una simple instalación de Orión NTA para mostrar, en general, el análisis de flujo y la función CBQoS de votación en Orión NTA. El Análisis de flujo y la realización de encuestas CBQoS ocurren simultáneamente: Flujo de dispositivos habilitados para enviar datos de caudal con el colector de Orión NTA en el puerto 2055, y las encuestas de Orión NTA colector CBQoS dispositivos habilitados para el tráfico de elaboración de políticas y resultados en el puerto 161.

Nota: CBQoS y el monitoreo de flujo se muestran por separado para enfatizar la diferencia en los métodos de recolección. Los extremos de la red no se muestran, y una típic instalación de Orion NTA no requeriría que todos los CBQoS y dispositivos capaces de flujo puede configurar para interactuar directamente con el colector de Orión NTA. Para obtener más información acerca de la implementación efectiva de NetFlow en la red, consulte la sección "Nuevas redes Volumen 3 - Conceptos básicos sobre NetFlow y estrategias de implementación".



Porque usar Orion NetFlow Traffic Analyzer (analizador de trafico de red Orion)

Orion NetFlow Traffic Analyzer le da la capacidad de forma rápida y sencilla de controlar los recursos de red y los patrones de uso a un nivel de detalle personalizable. Las siguientes valiosas características representan el núcleo de las capacidades de Orion NetFlow Traffic Analyzer:

Orion Alertas de Integración

Orion NTA agrega automáticamente información de hablador superior a las alertas de utilización de la interfaz. Usted puede navegar directamente a detalles de la interfaz NAT de los mensajes en el recurso de Eventos Orion.

Para obtener más información, vea Agregando Hablador Top Estadísticas a Alertas de Orión.

Gráficos personalizables tasa base

Cartas apiladas y gráficos de la zona nueva línea ofrecen opciones para incluir las estrías que muestra las tendencias de datos y opciones de gráficos incluyen ahora unidad de Tarifa (Kbps), porcentaje de la velocidad de la interfaz, por ciento del tráfico total, y los datos transferidos en cada intervalo.

Avanzada puerto y asignación de aplicación

Las asignaciones de aplicación pueden definirse sobre la base de las direcciones IP de origen y destino, además de puertos y protocolos.

Flujo de apoyo a la supervisión de Cisco Adaptive Security Appliances (ASA)

Orion NTA puede comunicar los datos de tráfico de red proporcionados por Cisco NetFlow habilitado para los dispositivos ASA.

Puntos de vista filtrados que incluyen tanto el ingreso y tráfico de la salida

Orion NTA ofrece ahora la posibilidad de seleccionar la dirección del tráfico en cualquier interfaz de vista. En cualquier interfaz de control, ahora pueden ver los datos de tráfico para el tráfico de entrada, el tráfico de salida, o ambos.

Soporte para dispositivos IPFIX

Protocolo de Internet de flujo de exportaciones es un estándar en desarrollo para el formato y transmisión de información de IP basado en el tráfico de red. A medida que más dispositivos cuentan con capacidad IPFIX, Orión NTA inmediatamente será capaz de proporcionar IPFIX monitoreo de flujo.

Clase de Cisco basado en la calidad del servicio (CBQoS) el seguimiento

Orion NAT proporciona recursos que le da la posibilidad de ver easiily, c corazón, e informar sobre los efectos de la calidad de la clase base de las políticas de servicio que ha habilitado en su CBQoS capaces dispositivos de Cisco.

Esta versión mejora CBQoS seguimiento con el apoyo parcial para las políticas anidadas y un control más granular sobre los dispositivos de votación específica.

Aumento de la disponibilidad y el rendimiento

Con Orion NTA, puede más rápidamente detectar, diagnosticar y resolver desaceleraciones y las interrupciones de la red.

Esta versión mejora la eficiencia CBQoS de votación, los tiempos de carga de los informes y vistas de resumen.

Planificación de la capacidad analítica

Orion NTA destaca las tendencias en el tráfico de red, lo que permite anticipar los cambios en el ancho de banda de forma inteligente a las áreas que están experimentando los cuellos de botella.

Esta versión incluye informes sobre conversaciones superiores con aplicaciones y puntos finales Top 50, y los recursos que muestra las fuentes de tráfico principales y Destinos de dominios, y Top IP Conversaciones Dirección del Grupo.

Red optimizada la asignación de recursos

Información proporcionada por Orion NTA le permite identificar y reasignar las áreas con exceso de capacidad de ancho de banda a zonas con conexiones limitadas o estresadas.

La alineación de los recursos de usted con las necesidades de negocio de la empresa

Debido a que Orion NAT se basa en la probada infraestructura Orion NPM, se puede evaluar tanto las necesidades de la red de la empresa en una visión de alto nivel y los detalles funcionales de las interfaces específicas y los ganglios.

Mayor seguridad de la red

Orion NTA le da la capacidad de forma rápida y precisa identificar el tráfico de red y exponer los patrones de curiosos, los comportamientos no deseados, y la utilización anómala que pueda indicar el posible virus, bot, o infección de spyware.

Soporte para múltiples puertos de flujo

El número y tipo de flujo de dispositivos disponibles han aumentado, por lo que el número de puertos sobre los que los datos de flujo se transmite también ha aumentado. Orion NTA es ahora compatible con la designación de varios puertos en los que los datos de flujo se pueden recibir.

Un todo en uno NetFlow, sFlow, J de flujo, y la solución de monitoreo IPFIX

Ahora usted puede parar el cambio entre paquetes de supervisión de la red para adquirir una imagen completa de la utilización, el rendimiento y las necesidades de su red, sin importar el tipo de registros de caudal proporcionado por los dispositivos de red diferentes.

Capítulo 2

Instalación de Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer (Orion NTA) cuenta con un procedimiento de instalación basada en asistente. Para un producto de clase empresarial, los requisitos son nominales.

Nota: Los datos NetFlow son extensos y puede consumir grandes cantidades de memoria de base de datos en un período relativamente corto de tiempo. Esto es cierto incluso para redes más pequeñas. Como resultado, SolarWinds requiere que la base de datos de SQL Server y el Orion NPM / instalación NTA se mantengan en servidores físicos independientes.

SQL Server y SQL Server Express con Orion NTA

Debido al hecho de que los datos NetFlow son extensos y pueden consumir grandes cantidades de memoria base de datos en un período relativamente corto de tiempo, SolarWinds no recomendamos el uso de instancias de SQL Server Express base de datos de Orion NTA. En cambio, SolarWinds recomienda el uso de una versión de producción de SQL Server.
Las evaluaciones de Orión NTA son una excepción limitada. Para fines de evaluación, Orion NPM y NTA Orion puede apoyar el uso de instancias de SQL Server Express 2005 de base de datos. SQL Server Express que permite evaluar Orion NTA con una base de datos real, y está disponible de forma gratuita, de Microsoft. Sin embargo, SolarWinds no recomienda su uso con Orion NTA en cualquier entorno de producción por las siguientes razones:

- SQL Server Express es incapaz de manejar bases de datos de más de 4 GB.
- SQL Server Express se limita a un solo procesador.
- SQL Server Express no puede utilizar más de 1 MB de RAM.

Nota: Para entornos de producción, instalaciones de NPM Orion y Orión NTA deben utilizar una instancia debase de datos SQL Server instalada en un servidor independiente (en un servidor separado).

Requerimientos

El servidor que se utiliza para alojar su solución debe ser compatible con NetFlow tanto Orion NPM y Orion Orion NTA NTA como se construye y amplía Orion NPM. En general, los requisitos para la versión actual de Orión NTA cumplen con los requisitos de un Orion NPM la versión 9.5 de instalación, según lo previsto en el "Orion NPM Requisitos" de la SolarWinds Orion Network Performance Monitor Guía del administrador.

Nota: De forma predeterminada, Orión NTA escucha los datos de flujo en el puerto 2055 (UDP). Asegúrese de que el puerto 2055 está abierto para la comunicación UDP en cualquier colector de Orión NTA

Requisitos de software

En las tablas siguientes se muestra una lista de los requisitos de software de la versión actual de Orión NTA.

Notas:

- Debido a la alta velocidad y grandes requisitos de memoria del control de las transacciones de flujo, Orion NTA y SQL Server deben ser instalado en servidores físicos independientes
- SQL Server Express y MSDE restringen el tamaño de cualquier base de datos de 4 GB y 2 GB, respectivamente. Por esta razón, SolarWinds no es compatible con el uso de cualquiera de SQL Express o MSDE con Orion NTA en entornos de producción.

Software	**Requirimientos**
Orion NPM	Version 9.5.1 o superior
S.O. (sistema operativo)	Windows 2008 Server (32-bit or 64-bit, con IIS en modo 32-bit) **Nota:** El servidor R2 de Windows 2008 ya no es soportado. Windows Server 2003 R2 (32-bits o 64 bits, con IIS en el modo de 32 bits) IIS debe estar instalado. SolarWinds Orion recomienda que los administradores del NPM tener privilegios de administrador local para asegurar la funcionalidad completa de herramientas locales Orion NPM. Cuentas limitadas al uso de la consola Web no requieren privilegios de administrador. **Nota**: SolarWinds no admite la instalación de Orion NPM en Windows XP o Vista en entornos de producción.
Servidor Web	Microsoft IIS, la versión 6.0 y posteriores, en el modo de 32 bits. Las especificaciones requieren que los nombres de host DNS se compongan de caracteres alfanuméricos (AZ, 0-9), el signo menos (-) (.), y períodos. Caracteres de subrayado (_) no están permitidos. Para obtener más información, vea RFC 952. **Nota**: SolarWinds no recomienda ni admite la instalación de Orión NTA en el mismo servidor o utilizar el mismo servidor de base como Research in Motion (RIM) servidor Blackberry.
.NET Framework	Version 3.5 o posterior

Software	Requirimientos
SNMP Trap Services (Servicios trampa)	sistema operativo Windows y el componente de gestión de herramientas de monitoreo
Consola de navegacion web	Microsoft Internet Explorer versión 6 o posterior con Active scripting Firefox 3.0 o posterior

SQL Server Software	Requerimientos
Sistema Operativo	Servidor Windows 2008 (32- or 64-bit) Servidor Windows 2003 R2, SP1 y superior (32- or 64-bit)
SQL Server (servidor SQL)	SQL Server 2005 SP1 Estandar o Empresarial SQL Server 2008 Estandar, o Empresarial **Nota:** Aunque SQL Server Express puede ser usado para los propósitos de evaluaciones se limitan a vigilar una o dos interfaces de SolarWinds muy poco tiempo; no se recomienda su uso para redes mas grandes.

Requerimientos de hardware

En la tabla siguiente se enumeran los requisitos mínimos de hardware para el seguimiento de una red típica con la versión actual de Orión NTA.

Nota: Orion NTA requiere que el puerto TCP 17777 está abierto tanto para enviar y recibir tráfico entre Orion NPM y los módulos de Orión otros.

Advertencia: Las configuraciones de RAID que sólo pueden utilizarse con Orion NTA son 0, 1, 0 +1 o 1 +0. Debido a la alta velocidad y grandes requisitos de memoria de datos NetFlow transacciones, SAN u otras configuraciones RAID no se debe utilizar, ya que pueden dar lugar a pérdidas de datos y disminuye significativamente el rendimiento.

Hardware	Requerimientos
CPU	3GHz o mas rapida, procesadores duales de doble núcleo.
RAM	3GB o mas.
Espacio en disco duro	**Orion NTA server:** 5GB o mas, RAID 0, 1, 01, o 10. Otras configuraciones RAID o SAN no son recomendables. **SQL Server:** 5GB o mas, RAID 0, 1, 01, o 10 en al menos 6 husillos. Otras configuraciones RAID o SAN no son recomandables.
Dispositivos NetFlow (flujo net)	Los dispositivos Cisco que utilizan la versión NetFlow 5 o 9 **Nota**: Orion NTA sólo reconoce la versión NetFlow nueve plantillas que incluyen todos los aspectos incluidos en la versión 5 de la plantilla de NetFlow.
Dispositivos IPFIX	Dispositivo red que use IPFIX
Dispositivos J-Flow	Dispositivo red que use J-Flow
Dispositivos sFlow	Dispositivo red que use sFlow version 5
Nota: Para obtener más información acerca de los flujos compatibles, vea "NetFlow, IPFIX, J	

Requisitos de la máquina virtual

Orion NTA puede ser instalado en máquinas virtuales VMware y Microsoft Virtual Server, si los requisitos cumplen con las siguientes por cada servidor virtual.

Configuracion de la máquina virtual	Requerimientos
Velocidad del CPU	3.0 GHz
Espacio del disco duro alocado	**Orion NTA server:** 5GB o mas, RAID 0, 1, 01, o 10. Otras configuraciones RAID o SAN no son recomendables. **SQL Server:** 5GB o mas, RAID 0, 1, 01, o 10 en al menos 6 spindles. Otras configuraciones RAID o SAN no son recomendables.
Memoria	2GB o mas
Interface de red	Cada instalación de Orion NPM debe tener su propia tarjeta de red dedicada. **Nota:** Desde que Orion NPM utiliza SNMP para supervisar la red, si usted no es capaz de dedicar una tarjeta de interfaz de red para su instalación Orion NPM, es posible que sea debido a las brechas en el monitoreo de datos debido a la baja prioridad que en general se asigna al tráfico SNMP.

Para obtener más información acerca de los requisitos de Orion NPM, consulte "Orion NPM Requisitos" en el *SolarWinds Orion Network Performance Monitor Administrator Guide*.

Requerimientos de NetFlow, IPFIX J-Flow, y sFlow

Cualquier paquete NetFlow, IPFIX, J-Flow, o sFlow que no incluyen los siguientes tipos de campo y los valores de campo puede ser ignorado por Orion NTA:

Field Type	Cantidad tipo de campo	Descripción
IN_BYTES	1	Entrada de contador de bytes
IN_PKTS	2	Los paquetes de ingreso contra
PROTOCOL	4	Layer 4 protocol
L4_SRC_PORT	7	Fuente puertos TCP/UDP
IPV4_SRC_ADDR	8	Dirección IP de origen
INPUT_SNMP	10	Entrada de interfaz de indice SNMP
L4_DST_PORT	11	Destino puertos TCP/UDP
IPV4_DST_ADDR	12	Destino de direccion IP
OUTPUT_SNMP	14	interfaz de salida del índice de SNMP

Notas:

- Sólo un índice de la interfaz es absolutamente necesario, pero ambos índices de interfaz (`INPUT_SNMP` y `OUTPUT_SNMP`) deben proveer una vista de estadísticas precisas, tanto para los flujos de entrada y salida.
- El tipo de campo SRC_TOS (número de campo de tipo 5) es necesario para ver el tipo de datos de servicio para el tráfico de más de una fuente de flujo, pero la plantilla utilizada por Cisco Adaptive Security Appliances (ASA) no proporciona este campo.
- Si SolarWinds establece que Orion NAT admite el control de flujo para un dispositivo, por lo menos una de las plantillas de las exportaciones del dispositivo cumple con estos requisitos.

Instalando Orion NetFlow Traffic Analyzer (Analizador de trafico de red Orion)

Realice el siguiente procedimiento para instalar Orion NTA. Usted debe proporcionar su puerto de NetFlow Traffic (su puerto de trafico de redes) y confirmar que está activado y enviando datos de NetFlow tráfico con el fin de completar la instalación.

Nota: El procedimiento siguiente supone que Orion NPM versión 9.5.1 o posterior ya está instalado en el servidor designado Orion NTA. Si desea evaluar Orion NPM, contactece con SolarWinds en sales@solarwinds.com.

Para instalar Orion NetFlow Traffic Analyzer:

1. Inicie sesión en el servidor Orion NPM que desea utilizar para el análisis de tráfico NetFlow.
2. ***Si estas instalando Orion NTA en un servidor terminal,*** complete los siguientes pasos antes de continuar con la instalacion de Orion NTA :
   a. Click **Start > Control Panel > Add or Remove Programs (start > panel de control > añadir o remover programas)**.
   b. Click **Add New Programs (añadir nuevos programas)**.

c. Click **CD or Floppy** (CD o Disquette)

d. Click **Next** (siguiente) en el programa de instalación desde el disco o disquette.

3. ***si usted descargó Orion NetFlow Traffic Analyzer del sitio web de SolarWinds,*** complete los siguientes pasos:

a. Navegue donde este localizado su archivo `.zip`

b. Extraiga el paquete de evaluación en un lugar apropiado.

c. Comienze el instalador ejecutable de SolarWinds Orion NTA.

4. ***Si usted recivió los medio físicos,*** complete los siguientes pasos:

a. Navegue donde este localizado su archivo `.zip`

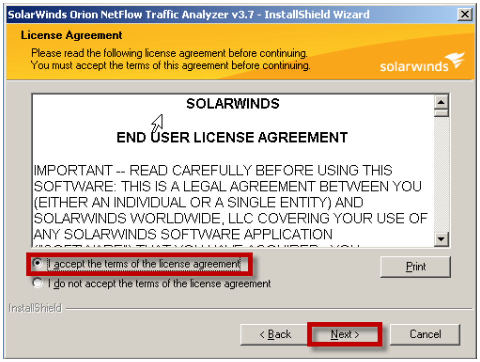
b. Extraiga el paquete de evaluación en un lugar apropiado.

c. Comienze el instalador ejecutable de SolarWinds Orion NTA.

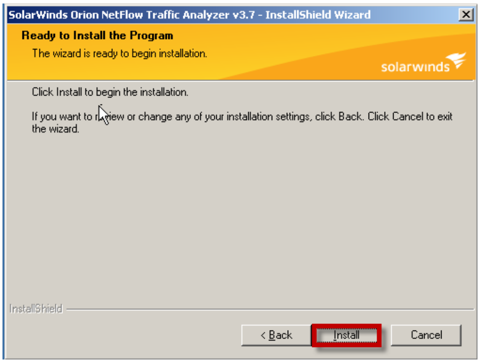
5. Revise el texto de Bienvenida.

6. Click **Next**. (siguiente)

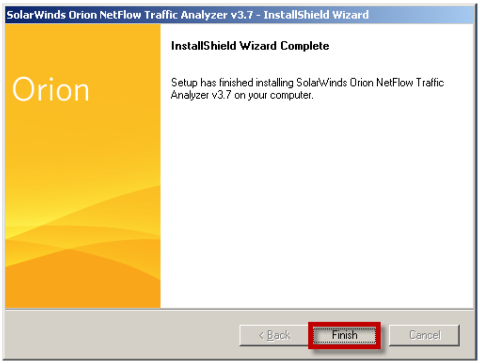
7. Selecciona **I accept the terms of the license agreement**, (yo acepto los terminus de lisencia) y luego haz click a **Next**.



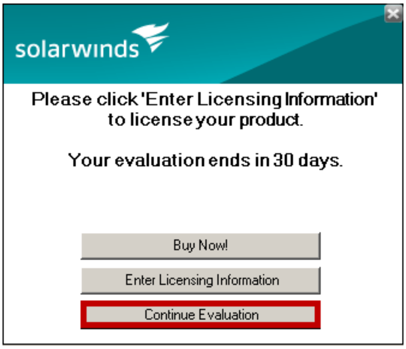
8. Click **Install** en la ventana de Ready to install the program “listo para instalar el programa”.



9. Cuando el asistente de instalacion finalice, haz click en **Finish** para salir del asistente.



10. Click **Continue Evaluation**.



11. **Si se le pide reiniciar el servidor,** seleccione una de las siguientes opciones, según corresponda:

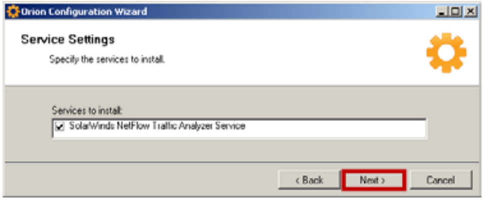
- ***Si estas instalando Orion NTA en un servidor terminal,*** click **No**.

- ***Si usted NO esta instalando Orion NTA en un servidor terminal,*** click **Yes**.

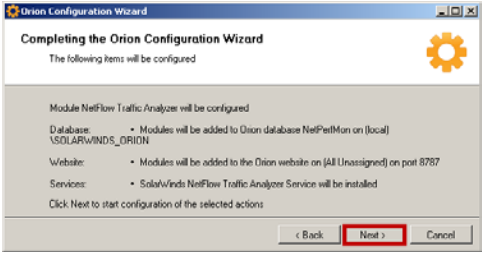
12. ***Si el asistente de configuracion no se inicia automaticamente, haz*** click en : **Start > All Programs > SolarWinds Orion > Configuration Wizard**.
13. Revisa el texto de bienvenida y luego haz click en: **Next**.



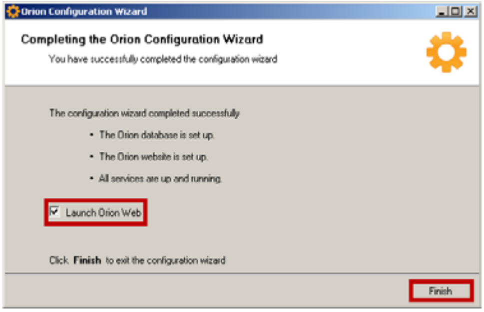
14. Confirme que el servicio de **SolarWinds NetFlow Traffic Analyzer** esta marcada en la ventana de configuración de servicio " Service Settings", y luego haz clic en **Next**.



15. Revise el resumen de configuración, a continuación, haz click en siguiente.



16. Después de que el Asistente para la configuración esté completo, confirman que el lanzamiento de Orión Web está marcado, y haga clic en **Finish (**Finalizar).



17. Entra en la consola Web de Orion como un administrador.

Nota: Si usted aún no le ah configurado otra contraseña de adiministrador, puede iniciar sesion con el ID del usuario `Admin` y sin contraseña.

18. ***Si se le pide para agregar recursos NetFlow a la pagina web de orion, haz*** click en: **Add Resources**.

Habilitacion de analisis de flujo de NTA Orion

Para comenzar a analizar los datos disponibles de caudal producido por los dispositivos dentro de su red, debe agregar un flujo habilitado de interfaz a la base de datos de Orión o el monitor de una interfaz previamente agregado que es capaz de generar los datos NetFlow. Añadir dispositivos NetFlow y las interfaces con la base de datos de Orión y la adición de los dispositivos e interfaces de NetFlow a Orion NetFlow NTA como fuentes son procedimientos específicos, detallados en secciones separadas, según se indica.

Preparación para la colecta de flujo de datos

Antes de intentar instalar Fuentes NetFlow a Orión NAT, configura cada dispositivo de red correspondientes a la exportación de datos de flujo de Orión NTA.

Para prepararse para la recolección de flujo:

1. Configurar los dispositivos de red para exportar los datos relativos a cada interfaz de referencia.

Consulte la documentación de los proveedores de su modelo. Hay algunos ejemplos en el Apéndice B de la Guía del administrador del analizador de trafico de redes Orion sobre la configuración de flujo de Cisco, Foundry, Extreme, y los dispositivos de HP.

Para obtener información sobre cómo habilitar NetFlor de los switches Cisco Catalyst, consulte **this SolarWinds technical reference paper**.

Para obtener información sobre como habilitar NetFlow en dispositivos Cisco ASA, consulte **this SolarWinds Knowledge Base article**.

2. Compruebe que cada interfaz que desea recibir y ver los datos que se están supervisando activamente en Orion NPM

Para esta tarea, para cualquier interfaz que es necesario agregar en Orion NPM, consulte Network Discovery Using Sonar Wizard (Deteccion de redes usando el asistente Sonar) en la guía de administrador de asistente en la SolarWinds Orion NPM.

3. Utilice una herramienta de captura de paquetes (por ejemplo, WireShark) en la interfaz y el Puerto correspondiente para verificar que el dispositivo es, de hecho, la exportacion de datos como se esperaba.

Añadiendo dispositivos y interfaces a la base de datos de Orion

El siguiente procedimiento añade una interfaze y sus interfaces con la base de datos de Orion usando la Web del nodo de administración de las características de la consola Web de Orión. Si el dispositivo NetFlow ya está configurado para enviar datos NetFlow, Orión NTA comenzará a recibir datos NetFlow tan pronto como el dispositivo se agrega a la base de datos de Orión.

Nota: Para obtener más información acerca de la designación de fuentes en Orion NetFlow NAT, consulte "Adición de fuentes de NetFlow de NetFlow Traffic Analyzer" en la página 19.

Para agregar flujo de dispositivos e interfaces a la base de datos de Orión:

1. Inicie sesión en el servidor que aloja Orion NPM de la instalación NTA.

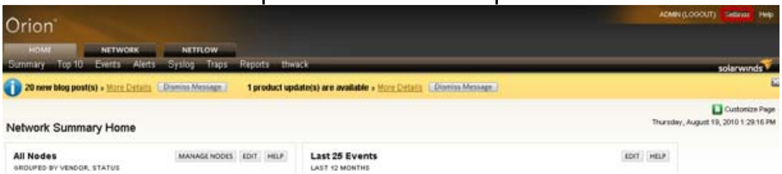
2. Click **Start > SolarWinds Orion > Orion Web Console**.

3. Inicie session en la pagina web de la consola Orion como un administrador.

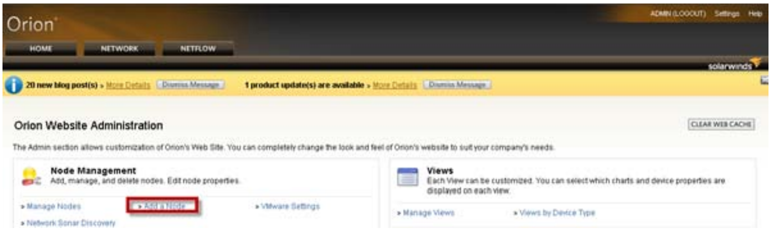
   Nota: Si aun no te haz creado otra contraseña de administrador, se puede acceder con la (ID de usuario) **User ID** `Admin` y sin contraseña.



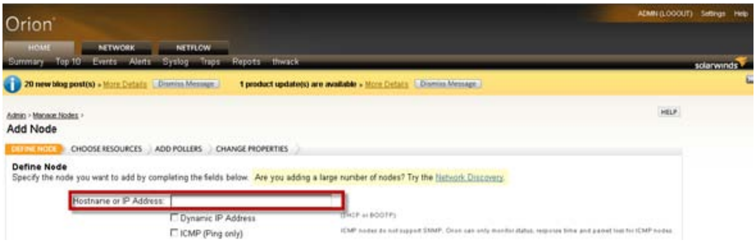
4. Click **Admin** en la esquina derecha de la pantalla-



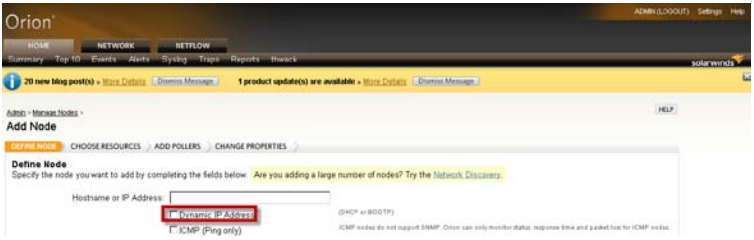
5. Click **Add a Node** en la gestión del nodo de agrupación.



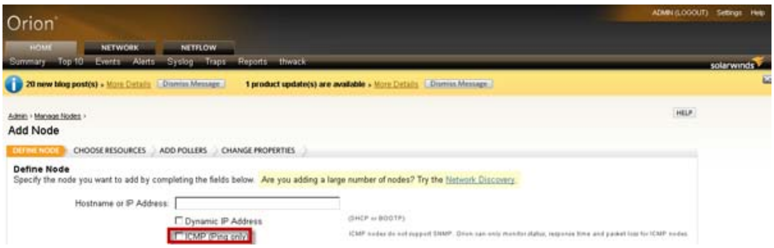
6. Proporcionar el nombre de host o dirección IP del flujo activado al dispositivo que desea agregar en el **Hostname or IP Address** (nombre de host o en el campo Dirección IP)



7. ***Si la direccióm IP del dispositivo que está agregando es asignada dinamicamente (DHCP or BOOTP),*** activa **Dynamic IP Address (dirección dinamica de IP)**.

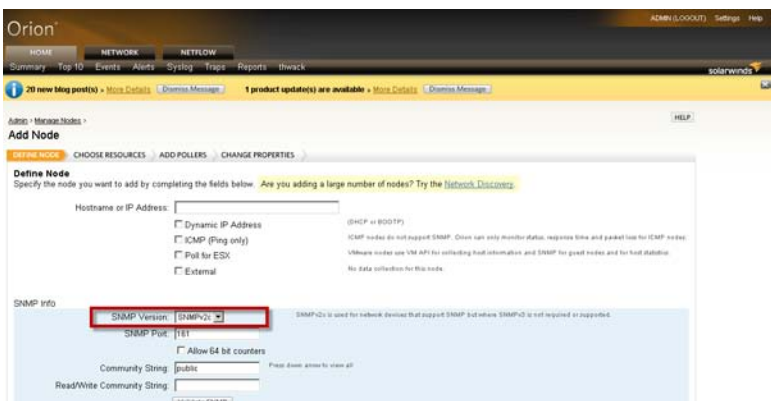


8. Confirma que **ICMP (Ping solo)** no esta activado.



9. Selecciona la **SNMP Version** (version SNMP)para el nodo añadido.

   Nota: Orion NPM utiliza **SNMPv2c** de forma predeterminada. Si su nuevo dispositivo admite o requiere las características de seguridad mejorada de SNMPv3, seleccione **SNMPv3**.



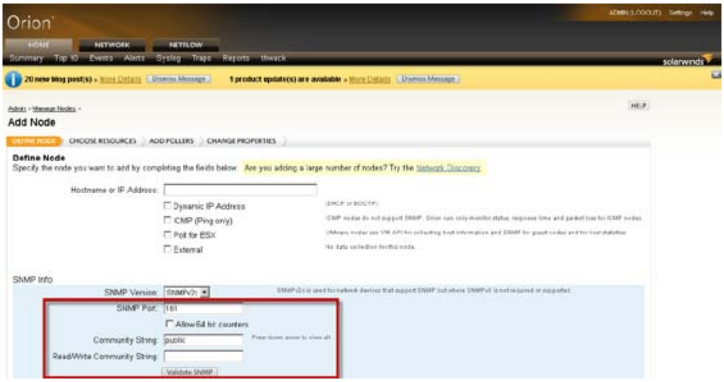
10. ***Si usted seleccionó* SNMPv2c,** siga los siguientes pasos:

a. ***Si el puerto SNMP en el nodo añadido no esta en el Orion NPM por defecto de 161,*** proporcionar el número de puerto real en el campo puerto SNMP.

b. ***Si el nodo añadido soporta contadores de 64-bit y usted quiere uasrlos,*** selecciona **Allow 64 bit counters (permitir contadores de 64 bits)**.

c. Proporciona cadenas de comunidad válida para el nodo añadido.

Nota: La **Read/Write Community String (cadena de comunidad de lectura/escritura)** es opcional, pero Orion NPM require de la cadena publica `public` de la comunidad,” **Community String “,** al mínimo.



11. ***Si usted selecciona* SNMPv3,** completa los siguientes pasos:

a. ***Si el puerto SNMP en el nodo añadido no es el de por defecto,*** proporcione el numero del puerto en el campo **SNMP Port** field.

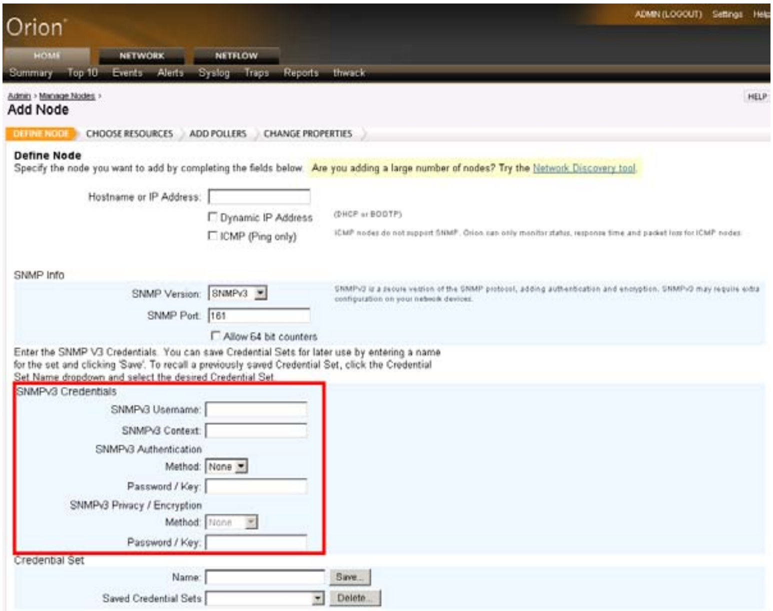
b. ***Si el nodo añadido soporta contadores de 64-bit y usted quiere uasrlos,*** selecciona **Allow 64 bit counters (permitir contadores de 64 bits)**.

Nota: Orion NPM es totalmente compatible con el uso de contadores de 64 bits, sin embargo, estos contadores de alta capacidad puede mostrar un comportamiento errático en función de la aplicación del fabricante. Si observa los resultados peculiares cuando se utiliza estos contadores, utilice los detalles de nodo para deshabilitar el uso de contadores de 64 bits para el dispositivo y entre en contacto con el fabricante del hardware.

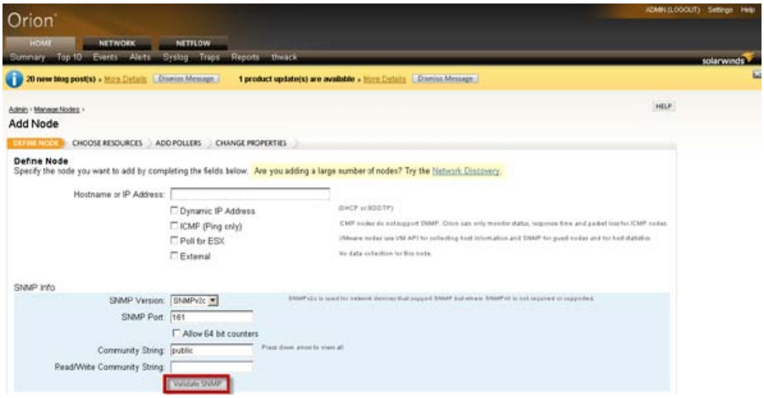
c. Proporciona los siguientes **SNMP Credentials (credenciales SNMP)** , **Authentication (autenticacion)**, y **Privacidad/configuración de cifrado**:

- **SNMPv3 Username (nombre de usuario)** y **SNMPv3 Context (contexto)**
- **SNMPv3 Authentication Method (método de autenticación)**
- **SNMPv3 Authentication Password/Key (autenticación de contraseña y clave)**
- **SNMPv3 Privacy/Encryption Method (privacidad metodo de cifrado)**
- **SNMPv3 Privacy/Encryption Password/Key (privacidad / cifrado de contraseña / clave)**

Note: A los efectos de esta evaluación, no son requeridas **Credenciales SNMPv3 de lectura/escritura**, y se asume que usted no tiene un conjunto de credenciales guardadas.



12. Click **Validate SNMP** (validar SNMP) después de entrar en todas las credenciales necesarias SNMP.



13. Después de confirmar que todas tus credenciales SNMP son validas, click **Next (siguiente)**.

14. Selecciona las interfaces que quieres que Orion NTA monitoree, y luego haz click en **Next**.

    Nota: Si usted no sabe cual es su flujo de interfaces habilitada, click **All Interfaces (todas las interfaces)**.



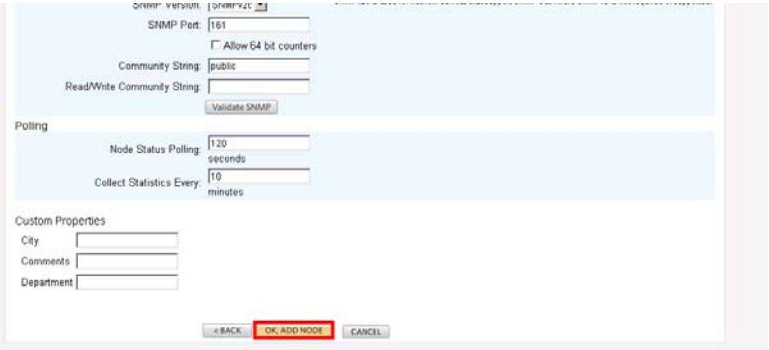
15. A los efectos de esta evaluación, click **Next** en la lista de añadir vista pollers.

    Nota: Para obtener mas informacion sobre el uso o la definicion de pollers, consulte la, *SolarWinds Orion Network Performance Monitor Administrator Guide (Guia del administrador del monitor administrador de performance de redes de SolarWinds Orion)*.

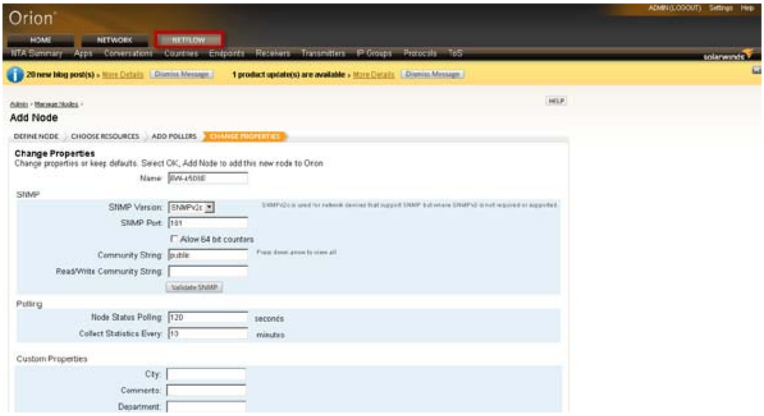


16. Click **OK, Add Node** (añadir nodo) en la vista de cambio de propiedades.

Nota: En este punto de vista, puede optar por proporcionar valores para las propiedades personalizadas predeterminadas: Ciudad, Comentarios, y el Departamento. Para obtener más información sobre el uso de las propiedades personalizadas, consulte "Creación de Propiedades" en el SolarWinds Orion Network Performance Monitor Guía del administrador.



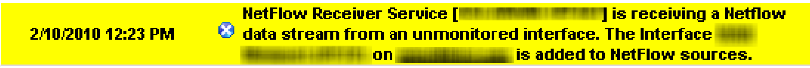
17. Click **OK** en el dialogo, y luego haz click en **NetFlow** en la barra de herramientas.



La siguiente sección proporciona los pasos necesarios para empezar a recibir datos NetFlow de flujo dispositivos en la red.

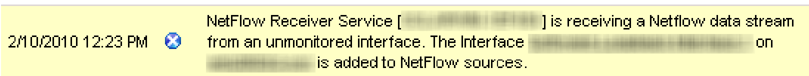
Agregar automáticamente Flujo y dispositivos CBQoS-habilitados

Orion NTA puede añadir automáticamente flujo y dispositivos habilitados CBQoS como fuentes NetFlow si están configurados para enviar los flujos a su designado servidor NAT Orión, como se muestra en el siguiente mensaje desde el pasado 25 de Análisis de Tráfico Eventos de recursos



.

NPM Orion también ofrece el siguiente mensaje en los últimos 25 eventos de recursos cuando se detecta una fuente, y añadió:



De forma predeterminada, en nuevas instalaciones, dispositivos de flujo de la red, se detectan y agregan automáticamente como fuentes NetFlow. Para obtener más información acerca de la gestión de los nuevos dispositivos de red, consulte "Añadiendo dispositivos y interfaces a la base de datos de Orion" en la página 16. Para obtener más información sobre la configuración de los dispositivos de flujo está activado, consulte "Ejemplos de configuración de dispositivos" en el SolarWinds Orion NetFlow Traffic Analyzer Guía del administrador.

Añadir NetFlow Sources (recursos de flujo de red) a NetFlow Traffic Analyzer (analizador de trafico de flujo de redes)

Después de que su flujo dispositivo activado y sus interfaces se han añadido a Orion NPM, debe designar el dispositivo como una fuente de NetFlow. El siguiente procedimiento proporciona los pasos necesarios para añadir fuentes a Orion NetFlow NTA.

Nota: Orion NTA sólo reconoce la versión NetFlow nueve plantillas que incluyen todos los campos utilizados por la versión NetFlow 5. Para obtener más información acerca de las plantillas de Orion NetFlow NTA reconoce, consulte "NetFlow, IP-FIX, J-Flow, y requisitos sFlow" en el SolarWinds Orion NetFlow Traffic Analyzer Guía del administrador.

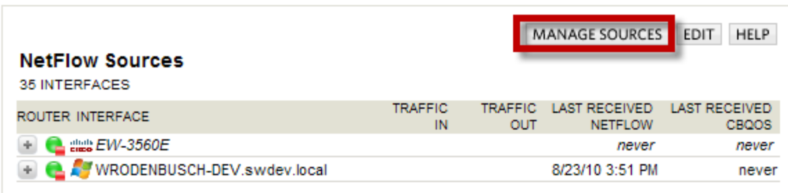
Para añadir dispositivos NetFlow y interfaces a NetFlow Traffic Analyzer:

1. Inicia sesión en el servidor de Orion NPM que aloja Orion NetFlow Traffic Analyzer.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.

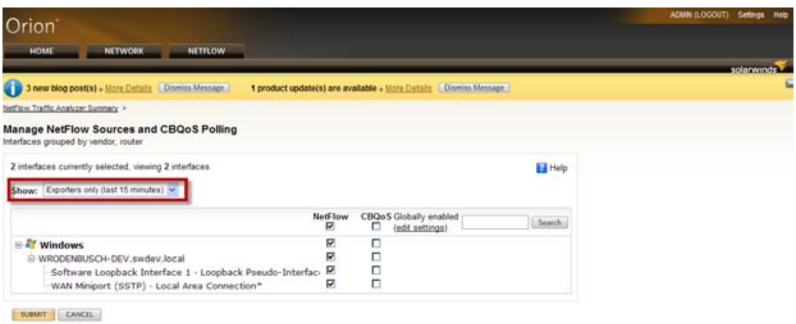
3. Inicia sesión en la consola web de Orion Web como un administrador.



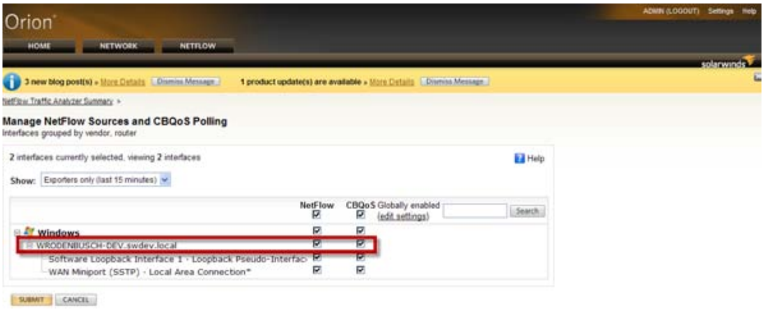
4. Click **Manage Sources** (gestionar recursos) en el encabezado de **NetFlow Sources**.



5. Selecciona **Exporters Only "sólo los exportadores" (dura 15 minutes)** del menu listado.



6. Expande la lista de dispositivos para ver todos los nodos de control, marque las opciones (**NetFlow** y / o **CBQoS**) para los nodos principales de las interfaces que desea Orion NTA para supervisar y, a continuación, haga click en **Send (enviar)**.



Orion NTA deben recibir los datos de tráfico y lo mostrará en pocos minutos.

Capítulo 3

Visita rápida a Orion NetFlow Traffic Analyzer

Las características y flexibilidad que ofrece Orion NetFlow Traffic Analyzer dan una visión altamente detallada de la cantidad y la calidad del tráfico en la red. Las secciones de este capítulo se basan en sí de forma secuencial para mostrar el resultado de las características clave de Orion NetFlow Traffic Analyzer. Este capítulo es más útil cuando es leído y seguido de principio a fin, el capítulo comienza con una visión general de los recursos disponibles de inmediato en el punto de vista de análisis de tráfico NetFlow Resumen, y continúa a través de los resúmenes de las más utilizadas puntos de vista de Orión NTA.

Nota: El uso extensivo de los casos, incluyendo los escenarios de la incorporación de otras herramientas de SolarWinds , están disponibles en el último capítulo de esta Guía de Evaluación. Para obtener más información, consulte "Uso de Orion NetFlow Traffic Analyzer" en la página 51.

Iniciando Orion NetFlow Traffic Analyzer

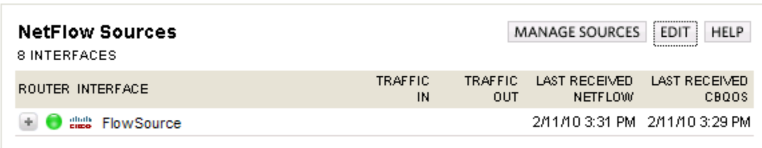
Para activar Orion NetFlow Traffic Analyzer, click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**. Para obtener más información acerca de la instalación y configuración de Orion NAT, consulte "Instalación de Orion NetFlow Traffic Analyzer" en la página 7.

Resumen de NetFlow Traffic analazer (analizador de trafico de red)

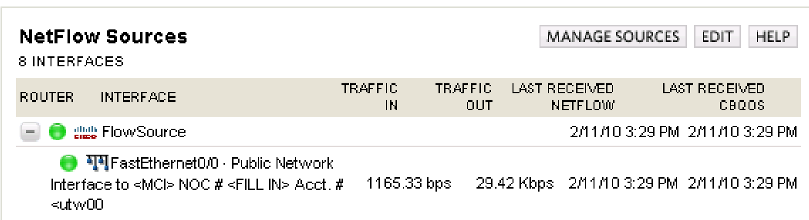
Al iniciar Orion NetFlow Traffic Analyzer, el Resumen del análisis de tráfico NetFlow es la primera vista que aparecera. Este punto de vista da una idea de las condiciones de tráfico de datos en toda la red. Los siguientes recursos están incluidos en el análisis de tráfico NetFlow la vista del resumen de forma predeterminada.

Fuentes NetFlow

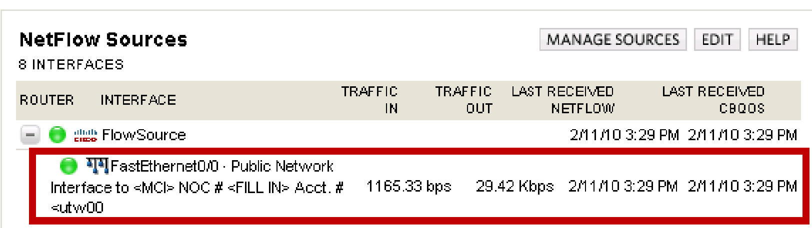
Este recurso proporciona una lista de todos los flujos y dispositivos CBQoS de la red que están actualmente configurado para enviar datos NetFlow al servidor que aloja su instalación de Orion NTA. Para obtener más información sobre cómo agregar los dispositivos de flujo está activado, consulte la sección "Habilitacion de analisis de flujo de NTA Orion" en la página 15.



Click **+** next (siguiente) a cualquier nombre de router para mostrar flujo y interfaces CBQoS habilitadas en el router seleccionado.



Las interfaces listadas aparecen tanto con un icono de estado y una marca de tiempo que indica cuando Orión última NTA recibido datos NetFlow de la interfaz seleccionada. Además, el recurso de NetFlow Fuentes proporciona valores reportados para el tráfico entrante y saliente en cada interfaz.

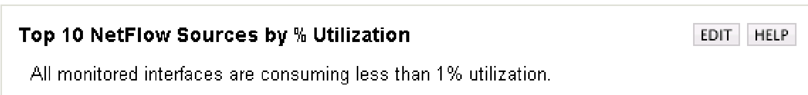


Al hacer clic en un nombre de router abre el Nodo opinión de los detalles NetFlow, y haciendo clic en un nombre de interfaz abre la interfaz de NetFlow vista Detalles. Para obtener más información acerca de la opinión de NetFlow Detalles de nodo, vea "NetFlow Nodo Ver detalles" en la página 43. Para obtener más información acerca de la opinión de la interfaz de NetFlow detalles, consulte "Ver detalles de la interfaz de NetFlow" en la página 48.

Top 10 NetFlow Fuentes por % de Utilización

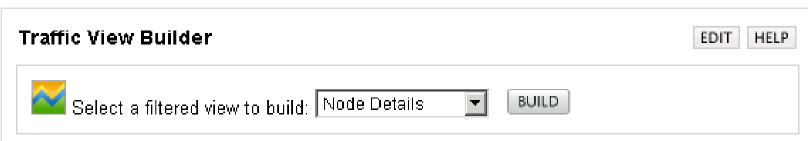
Este recurso proporciona una lista de las fuentes de NetFlow de la red que están actualmente de enrutamiento de tráfico suficiente para sus recursos de manera significativa del sistema tributario.

Nota: Las fuentes sólo aparecen si la experiencia de utilización es de más de 1%.



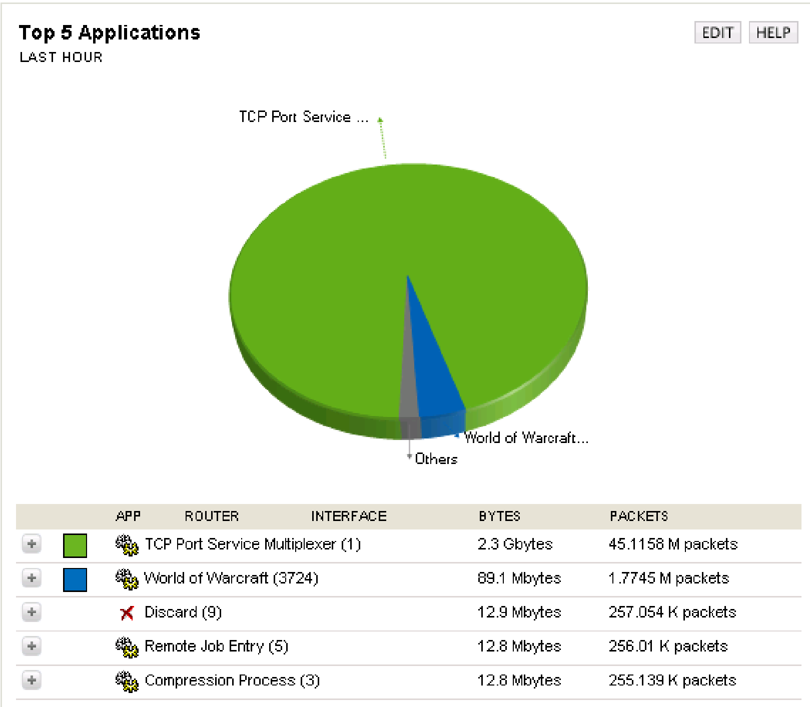
Traffic View Builder

La vista de tráfico Builder le permite crear tus propias opiniones Orion NTA. Debido a que Orion NTA es un módulo basado en web, puede crear favoritos del navegador de cualquier punto de vista de Orión NTA comprobar fácilmente el estado de los puntos problemáticos potenciales en una fecha posterior. Para obtener más información sobre el Generador de vista de tráfico, consulte "Uso de Orion NetFlow Traffic Analyzer” on page 51.



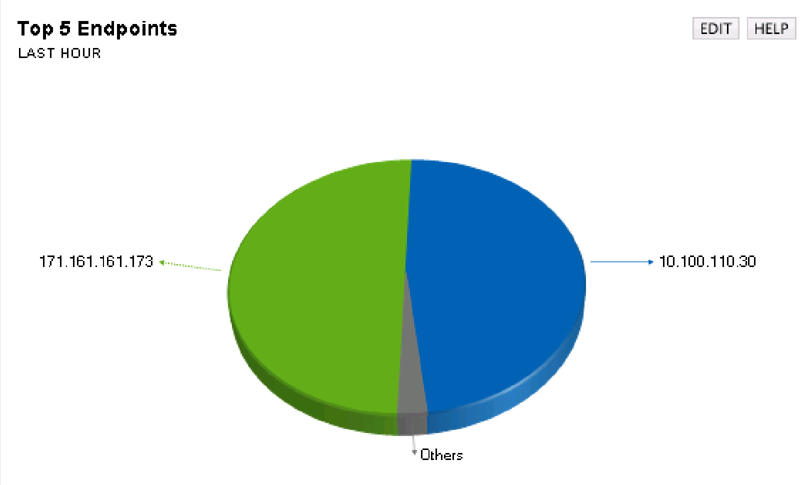
Top 5 aplicaciones

El Top 5 de los recursos de aplicaciones proporciona una vista rápida de las aplicaciones y los puertos que la mayoría están en uso por los dispositivos de la red. Al hacer clic en +, puede expandir cada aplicación para ver los dispositivos de red de enrutamiento de tráfico para cada aplicación.



Top 5 Puntos finales

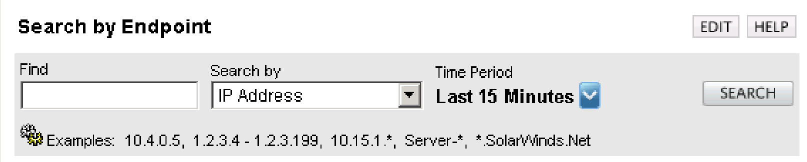
El Top 5 de los recursos extremos da una mirada a un punto de vista de los extremos que son las fuentes o destinos de la mayor parte del tráfico de red. Al hacer clic en + para expandir cada extremo, se puede ver los dispositivos de red de enrutamiento de tráfico para cada punto final.



		ENDPOINT	ROUTER	INTERFACE	BYTES	PACKETS
+	■	www.bankofamerica.com (171.161.161.173)			2.7 Gbytes	54.3713 M packets
+	■	10.100.110.30			2.6 Gbytes	51.8991 M packets
+		apacetti2-dev.tul.solarwinds.net (10.110.62.30)			103.4 Mbytes	2.0605 M packets
+		10.100.110.36			12.6 Mbytes	250.229 K packets
+		10.100.110.33			12.5 Mbytes	250.14 K packets

Búsqueda por punto final

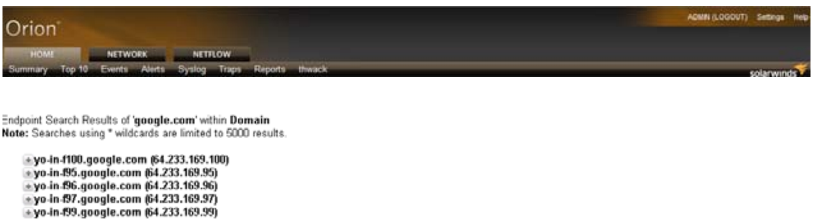
El uso de este recurso, puede localizar rápidamente cualquier extremo de la comunicación con los dispositivos de la red.



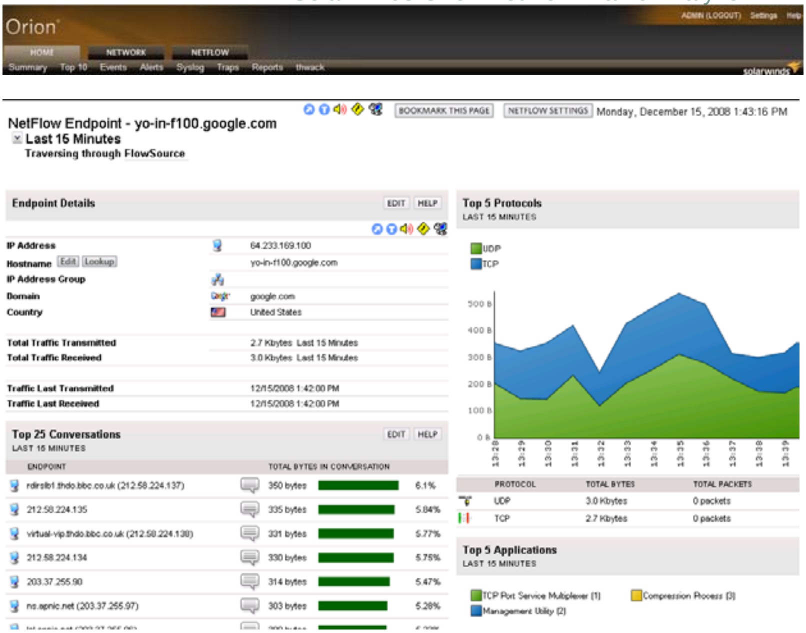
Sólo tiene que buscar para los puntos finales mediante el uso de cualquiera de los criterios en la tabla siguiente:

Search by Endpoint Criteria		
Country	Domain	Hostname
IP Address	IP Address Group Name	

Seleccione un periodo de tiempo, proporciona la identificación de un término de búsqueda y, a continuación, haga clic en **search** “buscar”. Los resultados de su búsqueda se presentaran en una lista expandible de los dispositivos de la red que son de enrutamiento de tráfico hacia o desde puntos finales coincidentes con su criterio de búsqueda.

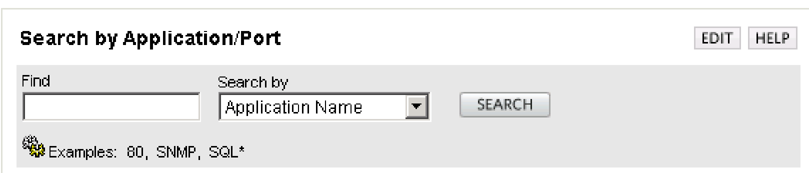


Al hacer clic en cualquier resultado, seguido haciendo clic en el nombre de cualquiera de sus dispositivos de red se abre la NetFlow Ver punto final para todo el tráfico de extremo a través del dispositivo seleccionado. Para obtener más información sobre Vista de NetFlow de punto final, consulte "NetFlow Endpoint View (vista de punto final de NetFlow)" en la página 39.

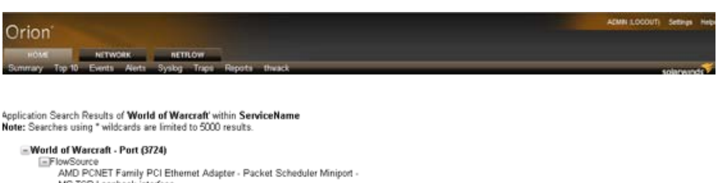


Búsqueda por aplicaciones / Puerto

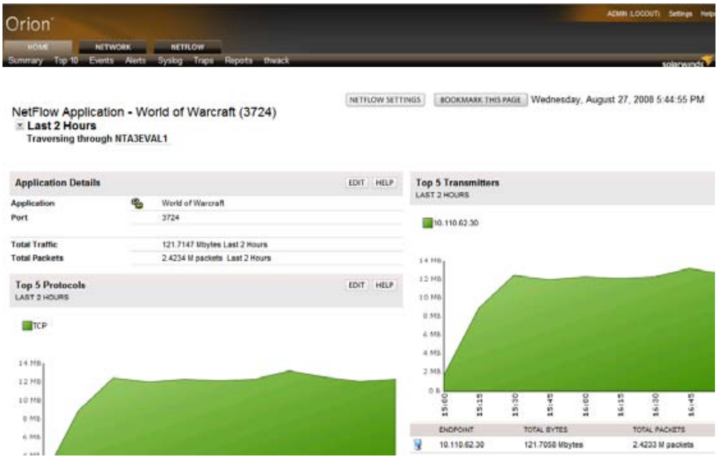
Con la Búsqueda por Aplicación / Puerto de los recursos, puede ver rápidamente los dispositivos de la red que estan utilizando una aplicación o un puerto en cualquier momento. Basta con elegir la búsqueda por nombre de la aplicación o el puerto, proporcionar un nombre de aplicación o el número de puerto y, a continuación, haga clic en **Search** (buscar).

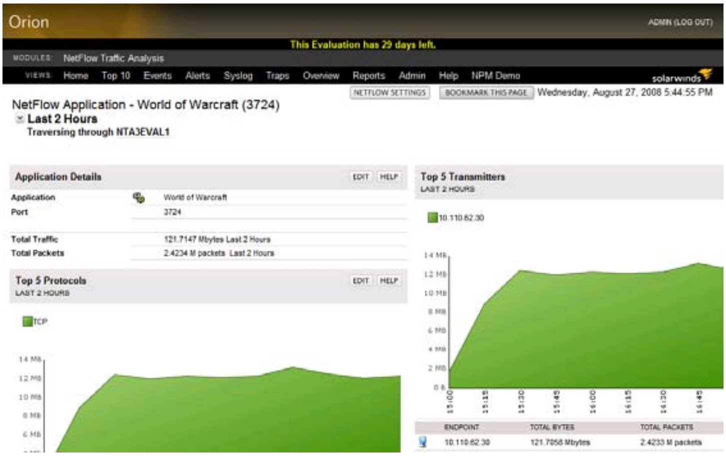


Los resultados de su búsqueda se presentarán en una lista expandible de los dispositivos de la red que son de enrutamiento de tráfico, ya sea para la aplicación seleccionada o sobre el puerto seleccionado.



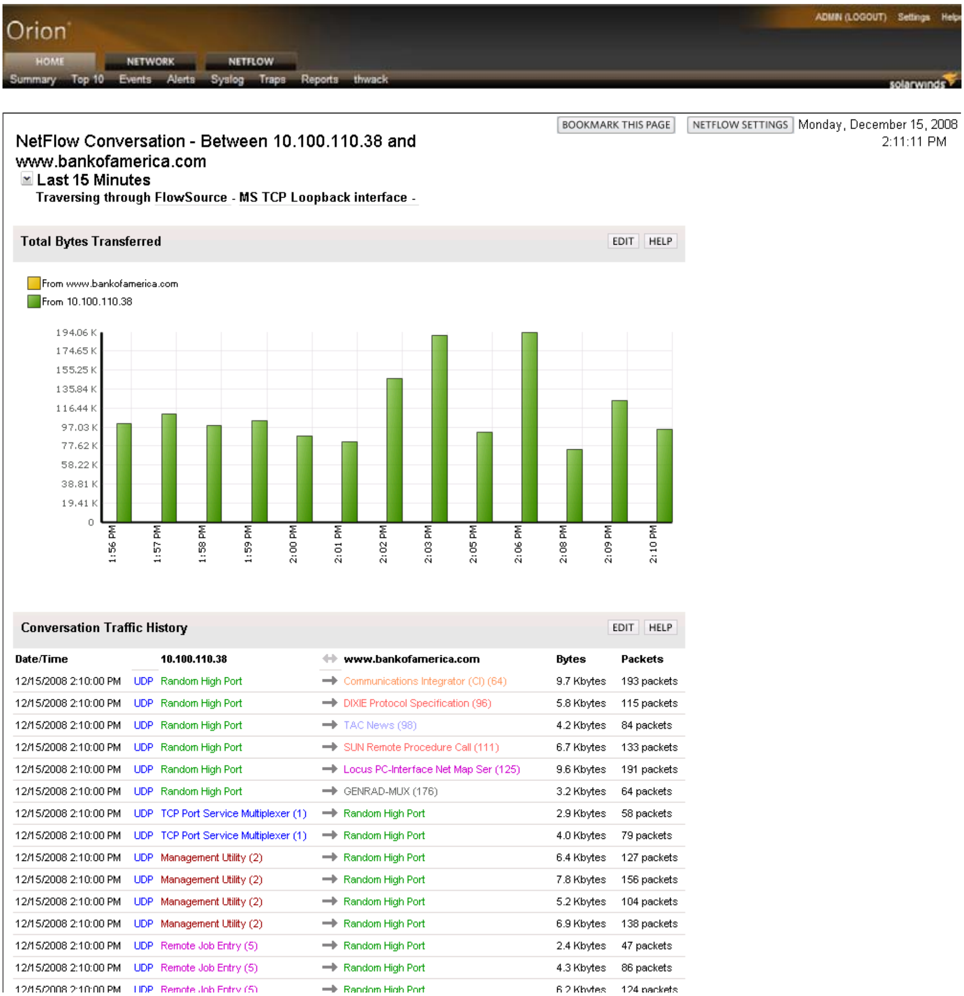
Haciendo clic en el nombre de un dispositivo de la red se abre la vista de aplicación NetFlow para todo el tráfico a través del dispositivo seleccionado que se destina a la búsqueda de la aplicación o enrutados a través del puerto buscado. Para obtener más información sobre Vista de NetFlow de aplicación, consulte "NetFlow Application View" en la página 37.

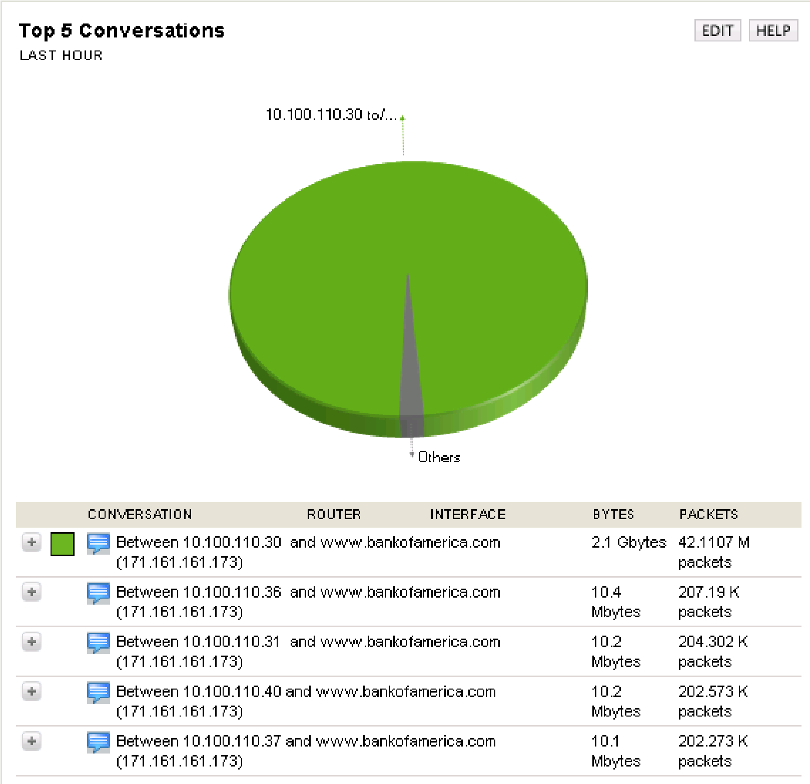




Conversaciones Top 5

Este recurso proporciona la vista de las conversaciones con el mayor ancho de banda de la red. Cada color de la tabla corresponde a una sola conversación continua entre dos extremos específicos. En la tabla del siguiente cuadro se enumeran los criterios de valoración que intervienen en cada conversación, con el ancho de banda consumido por cada conversación, en ambos: bytes y paquetes. Haga clic en + para expandir la descripción de conversación para ver todos los dispositivos de la red a través del cual se lleva a cabo la conversación seleccionada. El primer nivel de expansión muestra los nodos de red a través del cual se enruta el tráfico de conversación. El siguiente nivel de expansión muestra las interfaces que están de paso del tráfico de la conversación seleccionada.





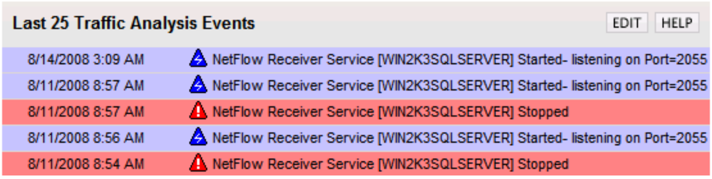
	CONVERSATION	ROUTER	INTERFACE	BYTES	PACKETS
+	Between 10.100.110.30 and www.bankofamerica.com (171.161.161.173)			2.1 Gbytes	42.1107 M packets
+	Between 10.100.110.36 and www.bankofamerica.com (171.161.161.173)			10.4 Mbytes	207.19 K packets
+	Between 10.100.110.31 and www.bankofamerica.com (171.161.161.173)			10.2 Mbytes	204.302 K packets
+	Between 10.100.110.40 and www.bankofamerica.com (171.161.161.173)			10.2 Mbytes	202.573 K packets
+	Between 10.100.110.37 and www.bankofamerica.com (171.161.161.173)			10.1 Mbytes	202.273 K packets

Tanto a nivel de nodo y la interfaz, las acciones respectivas del ancho de banda total consumido por la conversación seleccionada se muestran en los dos bytes y paquetes. Para cualquier nodo, el tráfico de conversación en el nodo es igual a la suma del tráfico de conversación en todas las interfaces en ese nodo.

Al hacer clic en el nombre de cualquier dispositivo de red se abre la NetFlow Vista de conversación para todo el tráfico entre los dos extremos de conversar a través del dispositivo de red seleccionado. Para obtener más información, consulte la sección "NetFlow Conversations View (vistas de conversaciones NetFlow)" en la página 41.

Analisador de tráfico de eventos

En este recurso se enumeran los últimos 25 eventos NetFlow específicos que se han producido a los dispositivos de la red monitoreada. Por lo general, en este recurso se enumeran las fechas y horas en el Servicio de NetFlow receptor se detiene y se inicia, pero también se utiliza para comunicar las actualizaciones de las actualizaciones de base de datos y de notificación de los nuevos fuentes de flujo descubiertos.



Vistas de Orion NetFlow Traffic Analyzer (analizador de tráfico de redes)

The following sections detail the types of information that are available by default on selected Orion NTA views.

Notas:

- Los siguientes son algunos de los puntos de vista de Orión NTA que se utilizan en la mayoría de instalaciones típicas. Estos puntos de vista mencionados están relacionados directamente de los recursos por defecto en la vista de análisis de tráfico NetFlow Resumen. Los recursos adicionales disponibles en el punto de vista de análisis de tráfico NetFlow Resumen y el posterior enlace Orion NTA vistas a vistas adicionales. Para obtener más información acerca de Orión opiniones NTA y recursos, consulte "Visualización de datos NetFlow Traffic Analyzer en la consola de Orión Web" en el SolarWinds Orion NetFlow Traffic Analyzer Guía del administrador.
- Algunos recursos pueden no estar presentes en la configuración predeterminada de una vista seleccionada. Para ver todos los recursos disponibles, debe modificar la vista desde el punto de vista de administración de la consola web Orion NPM. Para obtener más información, consulte "Visualización de datos NetFlow Traffic Analyzer en la consola de Orión Web" en el SolarWinds Orion NetFlow Traffic Analyzer Guía del administrador.

NetFlow Application View

The following sections offer brief descriptions of the resources on the default NetFlow Application view. More information about each resource, including configuration details, is available by clicking **Help** in the resource title bar.

Detalles de la aplicación

El recurso de Detalles de la aplicación proporciona una tabla que contiene la siguiente información sobre la aplicación y el puerto que está viendo en ese momento:

- Nombre de la aplicación
- Puerto usado por la aplicación
- Monto total de los datos de tráfico en el período de tiempo seleccionado
- Número total de paquetes enviados en el plazo de tiempo seleccionado

Top 5 de los protocolos

El Top 5 de los recursos de Protocolos proporciona una vista de los protocolos de tráfico de la aplicación seleccionadas mas usadas. En la tabla del siguiente cuadro proporciona el tipo de protocolo, la cantidad de datos, el número total de paquetes, y el porcentaje de todo el tráfico que ha estado utilizando cada protocolo en la lista.

Top 5 de tipos de servicios

El Top 5 Tipos de recursos de Servicios proporciona una visión de los servicios más activos empleados por la aplicación seleccionada. En la tabla del siguiente cuadro proporciona la siguiente información para cada tipo de servicio:

- El tipo de servicio
- La cantidad de trafico manejado por el servicio
- El número de paquetes manejado por el servicio
- El porcentaje de todo el tráfico de servicio a la aplicación seleccionada que se maneja por el tipo de servicio seleccionado

Bytes totales transferidos

El total de bytes transferidos muestra un recurso gráfico que detalla el número total de bytes que son transferidos por la aplicación seleccionada en un período determinado de tiempo. Una amplia gama de gráficos personalizados está disponible para imprimir o exportar de registros. Al hacer click se abre la tabla de la página de personalización del valor de la tabla seleccionada. Para obtener más información sobre la personalización de gráficos, consulte "Personalización de diagramas de NetFlow Traffic Analyzer" en el SolarWinds Orion NetFlow Traffic Analyzer Guía del administrador.

Unique visitors (Visitantes únicos)

El recurso de Visitantes únicos proporciona una tabla que detalla el número de direcciones IP únicas que han utilizado la aplicación seleccionada en un período determinado de tiempo. Una amplia gama de gráficos personalizados está disponible para imprimir o exportar de registros. Al hacer click se abre la tabla de la página de personalización del valor de la tabla seleccionada. Para obtener más información sobre la personalización de gráficos, consulte "Personalización de diagramas de NetFlow Traffic Analyzer" en el SolarWinds Orion NetFlow Traffic Analyzer Guía del administrador.

Total de paquetes transferidos (packages transferid)

El Total de paquetes muestra los recursos transferidos de un gráfico que detalla el número total de paquetes transferidos por la aplicación seleccionada en un período determinado de tiempo. Una amplia gama de gráficos personalizados está disponible para imprimir o exportar de registros. Al hacer click se abre la tabla de la página de personalización del valor de la tabla seleccionada. Para obtener más información sobre la personalización de gráficos, consulte "Personalización de diagramas de NetFlow Traffic Analyzer" en el *SolarWinds Orion NetFlow Traffic Analyzer Guía del administrador*.

Top 5 Transmitters (transmisores)

El Top 5 de los recursos de los Transmisores proporciona una visión de los extremos transmisores más activos mediante la aplicación seleccionada. En la tabla del siguiente cuadro proporciona la siguiente información para cada punto final:

- El nombre o la dirección IP del punto final
- La cantidad de tráfico que se transmite por el extremo
- El porcentaje del todo el tráfico de transmisión que es rastreable hasta el punto final

Puede hacer click en cada extremo de la lista para abrir la vista de NetFlow de extremos que se presentan estadísticas similares para cada extremo de la transmisión. Para obtener más información, consulte "NetFlow Endpoint View (vista de punto final de NetFlow)" en la página 41.

Top 5 Receivers (receptores)

El Top 5 de los receptores de recursos ofrece una visión de los extremos más activos que reciben mediante la aplicación seleccionada. En la tabla del siguiente cuadro proporciona la siguiente información para cada punto final:

- El nombre o la dirección IP del punto final
- La cantidad de tráfico que se recive por el extremo
- El porcentaje del todo el tráfico recivido que es rastreable hasta el punto final

Usted Puede hacer click en cada extremo de la lista para abrir la vista de NetFlow de extremos que se presentan estadísticas similares para cada extremo de recepción. Para obtener más información, consulte "NetFlow Endpoint View (vista de punto final de NetFlow)" en la página 41.

Top 5 de las Fuentes de tráfico por país

El Top 5 de las fuentes de tráfico por el recurso de Campo ofrece una visión de los países donde el tráfico en la aplicación seleccionada se origina, clasificadas según el porcentaje del tráfico total de la aplicación. En la tabla siguiente cuadro proporciona la siguiente información para cada país:

- El nombre del país
- La cantidad de tráfico que tiene su origen en el país
- El porcentaje de todo el tráfico que es rastreable al país

Top 5 Traffic Destinations by Country (destinos de tráfico por país)

El Top 5 destinos de tráfico por el recurso de Campo ofrece una visión de los países que sirven como destino del tráfico en la aplicación seleccionada, ordenados por el porcentaje del tráfico total de la aplicación. La tabla del siguiente cuadro proporciona la siguiente información para cada país:

- El nombre del país
- La cantidad de tráfico de aplicaciones que se dirige a los extremos en el país
- El porcentaje del total de tráfico de aplicaciones trazables a los extremos en el país

Top 5 Conversations (conversaciones)

El Top 5 de los recursos de Conversaciones proporciona una lista de las conversaciones más pesadas de ancho de banda en ruta a través del dispositivo seleccionado, mediante la aplicación seleccionada. Conversaciones que se encuentran con la cantidad de datos transferidos en la conversación, tanto en bytes y paquetes, y el porcentaje de tráfico de la aplicación total generado por la conversación. Al hacer clic en una conversación se abre la vista de NetFlow de conversación para la conversación seleccionada. Para obtener más información, consulte la sección "NetFlow Conversations View (vistas de conversaciones NetFlow)" en la página 41.

NetFlow Conversations View (vistas de conversaciones NetFlow)

Las siguientes secciones ofrecen una breve descripción de los recursos en la vista predeterminada conversaciones NetFlow. Más información acerca de cada uno de los recursos, incluidos los detalles de configuración, está disponible haciendo clic en Ayuda en la barra de título de los recursos.

Total de bytes transferidos

El total de recursos transferidos Bytes muestra un gráfico que detalla el número total de bytes transferidos, en un período determinado de tiempo, entre los dos nodos, las direcciones IP o dominios que se indica en el título de la vista.

Historial de conversaciones de tráfico

El recurso de conversación Tráfico Historia ofrece una tabla que muestra la siguiente información para cada intercambio de conversación en la lista:

- La fecha y hora de intercambios
- El protocolo utilizado para el intercambio
- La aplicación y el Puerto utilizado para el intercambio
- La direccion del flujo de trafico
- La cantidad de tráfico comunicado en bytes
- El número equivalente de paquetes comunicado

NetFlow Endpoint View (vista de punto final de NetFlow)

Las siguientes secciones ofrecen una breve descripción de los recursos en la vista predeterminada NetFlow extremo. Más información acerca de cada uno de los recursos, incluidos los detalles de configuración, está disponible haciendo clic en Ayuda en la barra de título de los recursos.

Detalles de EndPoint (punto final)

El recurso de Detalles de puntos finales prove de la siguientes información acerca del punto final seleccionado:

- Dirección IP
- HostName (Nombre de la máquina)
- IP address group (Direccion grupal)
- Domain (Dominio)
- Country (País)

- El trafico total transmitido y recibido
- Marcas de fecha y tiempo de los datos transmitidos y recibidos al final.

Top 25 Conversaciones

Este recurso proporciona una lista de los criterios de valoración con la que el punto final que se está viendo haya transferido la mayoría de los datos. Para cada conversación, este recurso informa de la cantidad de datos transferidos en la conversación y el porcentaje de la conversación listada representa el total de datos transferidos por el extremo de verse. Al hacer clic en un extremo se abre la vista de NetFlow de punto final para el punto final seleccionado. Todos los otros enlaces para un extremo que figuran abrir la vista de NetFlow de conversación para la conversación entre los extremos vistos y seleccionados. Para obtener más información, consulte la sección "NetFlow Conversations View (vistas de conversaciones NetFlow)" en la página 41.

Total Packets Transferred (total de paquetes trasferidos)

El Total de paquetes muestra los recursos transferidos en un gráfico con el número total de paquetes de transmisión, tanto desde el punto final visto y recibido por el extremo visto durante un período determinado de tiempo.

Bytes totales transferidos

El recurso de total de bytes transferidos muestra un gráfico que detalla el número total de bytes transmitidos, tanto desde el punto final visto y recibido por el extremo de ver, en un período determinado de tiempo.

Top 5 de protocolos

El recurso Top 5 de Protocolos ofrece una mirada de los protocolos de tráfico en un punto de vista de los puntos seleccionados según su cantidad de uso. En la tabla siguiente al cuadro se proporciona el tipo de protocolo, la cantidad de datos, el número total de paquetes, y el porcentaje de todo el tráfico que ha estado utilizando cada protocolo en la lista.

Top 5 Aplicaciones

El Top 5 de los recursos de aplicaciones proporciona una vista rápida de las aplicaciones utilizadas por la mayoría de la variable seleccionada. En la tabla del siguiente cuadro se proporciona el nombre de la aplicación, la cantidad de datos que está fluyendo, el número total equivalente de los paquetes, y el porcentaje de todo el tráfico que es detectable con el uso de la aplicación de la lista de la variable seleccionada. Al hacer clic se abre una aplicación de la vista NetFlow aplicación. Para obtener más información, consulte "NetFlow Application View" en la página 37.

Top 5 de las Fuentes de tráfico por país

El Top 5 de las fuentes de tráfico por el recurso de Campo ofrece una mirada en un punto de vista, en forma de un gráfico, de los países donde el tráfico hasta el punto final seleccionado es originario, clasificado por el porcentaje del tráfico total de la variable seleccionada. En la tabla siguiente al cuadro proporciona el nombre del país de abastecimiento de tráfico al extremo considerado, la cantidad de tráfico encaminado al extremo del país en la lista, y el porcentaje de todo el tráfico encaminado al extremo visto que es rastreable al país en la lista.

Top 5 destinos de tráfico por país

El Top 5 de destinos de tráfico por el recurso de Campo ofrece un gráfico y la tabla de los países anfitriones de los destinos del tráfico de la variable seleccionada, clasificada por el porcentaje del tráfico total de la variable seleccionada. En la tabla siguiente al cuadro proporciona el nombre del país al que se encamina el tráfico, la cantidad de tráfico a los servidores en el país en la lista, y el porcentaje de todo el tráfico dirigido desde el extremo visto que se dirige a los servidores en el país de la lista.

Unique Visitors (Visitantes Únicos)

El recurso de Visitantes únicos proporciona una tabla de direcciones IP únicas que se han comunicado con el extremo visto durante un período determinado de tiempo.

Los 5 mejores destinos del tráfico de dominios

El Top 5 de destinos de tráfico de los recursos por dominio proporciona un gráfico y la tabla de los dominios de alojamiento destinos del tráfico de la variable seleccionada, clasificada por el porcentaje del tráfico total de la variable seleccionada. En la tabla siguiente al cuadro proporciona el nombre del dominio al que se encamina el tráfico, la cantidad de tráfico a los servidores en el dominio de la lista, y el porcentaje de todo el tráfico dirigido desde el extremo visto que se dirige a los servidores en el dominio de la lista.

Top 5 Traffic Sources by Domain (Top 5 de las fuentes de tráfico de dominios)

El Top 5 de las fuentes de tráfico por los recursos de dominio proporciona un gráfico y una tabla de los dominios de alojamiento fuentes de tráfico desde el punto final seleccionado, clasificado por el porcentaje del tráfico total de la variable seleccionada. En la tabla siguiente al cuadro proporciona el nombre del dominio al que se encamina el tráfico, la cantidad de tráfico a los servidores en el dominio de la lista, y el porcentaje de todo el tráfico dirigido desde el extremo visto que se dirige a los servidores en el dominio de la lista.

Top 5 IP Group Conversations (Top 5 Conversacion grupo IP)

El recursoTop 5 de los grupos conversacionales de propiedad intelectual proporciona un gráfico y una tabla de las conversaciones de la generación de tráfico desde el punto final seleccionado, clasificado por el porcentaje del tráfico total. En la tabla siguiente al cuadro se proporciona el nombre del grupo de IP para el tráfico que se dirige, la cantidad de tráfico dirigida a los servidores de la lista del grupo de investigación, y el porcentaje de todo el tráfico dirigido desde el extremo visto que se dirige a los servidores de la lista Grupo IP.

Top 5 Types of Service (Tipos de servicio)

El recurso Top 5 de Tipos de Servicios proporciona una vista rápida de los servicios más activos trabajando de la variable seleccionada. En la tabla siguiente al cuadro se proporciona la siguiente información para cada tipo de servicio:

- El tipo de servicio
- La cantidad de trafico, en bytes y packets (paquetes), que es manejado por el servicio
- El porcentaje de todo el tráfico de servicio hasta el punto final seleccionado que es manejado por el tipo de servicio seleccionado

Para obtener más información acerca de la supervisión de tipo de servicio en Orión NAT, consulte "Configuración de NetFlow Tipos de servicios" en el *SolarWinds Orion NetFlow Traffic Analyzer Guía del administrador.*

Ver detalles de la interfaz de NetFlow

Las siguientes secciones ofrecen una breve descripción de los recursos en la vista predeterminada de interfaz de NetFlow Detalles. Más información acerca de cada uno de los recursos, incluidos los detalles de configuración, está disponible haciendo click en **Help** en la barra de título de los recursos.

Top 5 Protocolos

El recurso Top 5 de los Protocolos proporciona una vista de los protocolos de tráfico de la interfaces mas vistas. En la tabla siguiente al cuadro se proporciona el tipo de protocolo, la cantidad de datos, el número total de paquetes, y el porcentaje de todo el tráfico sobre la interfaz de ver con cada protocolo en la lista.

Top 5 Aplicaciones

El recurso Top 5 de aplicaciones proporciona una vista rápida de las aplicaciones más utilizadas por la interfaz de vista. En la tabla siguiente al cuadro se proporciona el nombre de la aplicación, la cantidad de datos que está fluyendo, el número total equivalente de los paquetes, y el porcentaje de todo el tráfico que es detectable con el uso de la aplicación de la lista de la interfaz de vista. Al hacer clic se abre una aplicación de la vista NetFlow aplicación. Para obtener más información, consulte "NetFlow Application View" en la página 37.

Top 5 Conversaciones

Este recurso proporciona una lista de las conversaciones de la creación de la mayor parte del tráfico sobre la interfaz de vista. Para cada conversación, este recurso informa de la cantidad de datos transferidos en la conversación y el porcentaje de la conversación lista representa del total de datos transferidos a través de la interfaz de vista. Al hacer clic en una conversación se abre la vista de NetFlow de conversación para la conversación seleccionada. Para obtener más información, consulte la sección "NetFlow Conversations View (vistas de conversaciones NetFlow)" en la página 41.

CBQoS Pre-Policy Class Map (CBQoS mapa clase pre-politico)

Si usted está viendo una interfaz CBQoS habilitada a la que una política CBQoS se aplica actualmente, este recurso muestra las clases de tráfico que atraviesa la interfaz vista. Para cada clase de tráfico definido, la tabla debajo del cuadro a continuación informa de los valores promedio de la interfaz; y de las interfaces encuestadas utilizadas mas recientemente como un porcentaje del ancho de banda total de la interfaz medida antes de cualquier tráfico de configuración de la política CBQoS aplicada en la interfaz vista.

CBQoS Drops (cae)

Si usted está viendo una interfaz CBQoS habilitada a la que una política CBQoS se aplica actualmente, este recurso muestra la cantidad de tráfico que atraviesa la interfaz vista **que se ha caído** como resultado de la aplicación de políticas CBQoS. Para cada clase de tráfico definido, la tabla debajo del cuadro a continuación informa de los valores promedio de la interfaz y de las interfaces encuestadas utilizadas más recientemente como un porcentaje del ancho de banda total de la interfaz definida que corresponde a la cantidad de tráfico que se ha caído como resultado de la aplicación de políticas CBQoS.

Top 5 Endpoints (Puntos finales o extremos)

El Top 5 de los recursos extremos ofrece una visión de los extremos de producción de la mayor parte del tráfico en la interfaz seleccionada. En la tabla siguiente al cuadro se proporciona el nombre o la dirección IP de cada extremo de la lista, la cantidad de tráfico de cada extremo de la lista, tanto en bytes y paquetes, y el porcentaje de todo el tráfico sobre la interfaz de vista que es atribuible a cada extremo de la lista. Al hacer clic en un extremo abre la vista NetFlow de punto final para el punto final seleccionado. Para obtener más información, consulte "NetFlow Endpoint View (vista de punto final de NetFlow)" en la página 41.

Top 5 Traffic Destinations by Domain (Los 5 mejores destino de tráfico de dominios)

El recurso Top 5 de destinos de tráfico de dominios proporciona un gráfico y una tabla de los dominios de alojamiento de destinos del tráfico de la interfaz seleccionada, ordenados por el porcentaje del tráfico total. En la tabla siguiente al cuadro se proporciona el nombre del dominio al que se encamina el tráfico, la cantidad de tráfico a los servidores en el dominio de la lista, y el porcentaje de todo el tráfico dirigido desde la interfaz de vista que se dirige a los servidores en el dominio de la lista.

Top 5 Traffic Sources by Domain (Top 5 de las fuentes de tráfico de dominios)

El recurso Top 5 de las fuentes de tráfico de dominio proporciona un gráfico y una tabla de los dominios de alojamiento de fuentes de tráfico de la interfaz seleccionada, clasificada por el porcentaje del tráfico total de la interfaz seleccionada. En la tabla siguiente al cuadro se proporciona el nombre del dominio al que se encamina el tráfico, la cantidad de tráfico a los servidores en el dominio de la lista, y el porcentaje de todo el tráfico dirigido desde la interfaz de vista que se dirige a los servidores en el dominio de la lista.

Top 5 IP Group Conversations (Top 5 Conversaciones Grupo IP)

El recurso Top 5 de los grupos conversacionales de propiedad intelectual proporciona un gráfico y la tabla de las conversaciones de la generación de tráfico de la interfaz seleccionada, clasificada por el porcentaje del tráfico total. En la tabla siguiente al cuadro se proporciona el nombre del grupo de IP para el tráfico que se dirige, la cantidad de tráfico dirigida a los servidores de la lista del grupo de investigación, y el porcentaje de todo el tráfico dirigido desde la interfaz de vista que se dirige a los servidores de la lista Grupo IP.

Top 5 Domains (Top 5 Dominios)

Este recurso proporciona una visión de los dominios que producen la mayor parte del tráfico en la interfaz seleccionada. En la tabla siguiente al cuadro se proporciona el nombre del dominio, la cantidad de tráfico en bytes, el número total de paquetes comunicado, y el porcentaje de todo el tráfico en la interfaz seleccionada que es atribuible a cada dominio.

Nota: Este recurso sólo está disponible si la resolución de DNS persistente está habilitada. De forma predeterminada en las instalaciones de evaluación, resolución de DNS está configurado para aparecer en la demanda solamente. Para obtener más información, consulte "Configuración de DNS y NetBIOS Resolución" en el *SolarWinds Orion NetFlow Traffic Analyzer Guía del administrador.*

Top 5 Types of Service (Tipos de Servicio)

El recurso Top 5 Tipos de Servicio proporciona una vista rápida de los servicios trabajadores mas activos de la interfaz de vista. En la tabla siguiente al cuadro se proporciona la siguiente información para cada tipo de servicio:

- El tipo de servicio
- La cantidad de tráfico, en bytes y **packeage** (paquetes), que es manejado por el servicio a través de la interfaz de vista
- El porcentaje de todo el tráfico de la interfaz vista que es manejado por el tipo de servicio seleccionado

Para obtener más información acerca de la supervisión del tipo de servicio en Orión NAT, consulte "Configuración de NetFlow Tipos de servicios" en el *SolarWinds Orion NetFlow Traffic Analyzer Guía del administrador*.

CBQoS Post-Policy Class Map (Mensaje CBQoS Mapa Clase Política)

Si usted está viendo una interfaz CBQoS habilitada a una política CBQoS que se aplica actualmente, este recurso muestra las clases de tráfico que atraviesa la interfaz vista. Para cada clase de tráfico definido, la tabla debajo del cuadro a continuación informa de los valores promedio de la interfaz; y de las interfaces encuestadas utilizadas mas recientemente como un porcentaje del ancho de banda total de la interfaz medida antes de cualquier tráfico de configuración de la política CBQoS aplicada en la interfaz vista.

Detalles de la política CBQoS

Si usted está viendo una interfaz CBQoS habilitada a la que una política CBQoS se aplica actualmente, este recurso muestra el tráfico de las políticas aplicadas y las correspondientes clases de tráfico definidas en la interfaz de vista. Para cada clase de tráfico, este recurso proporciona la cantidad de tráfico y el porcentaje correspondiente de ancho de banda total de la interfaz definida por tanto la última hora y las últimas 24 horas.

Ver detalles de la interfaz de NetFlow

Las siguientes secciones ofrecen una breve descripción de los recursos en la vista predeterminada de interfaz de NetFlow Detalles. Más información acerca de cada uno de los recursos, incluidos los detalles de configuración, está disponible haciendo click en **Help** en la barra de título de los recursos.

Top 5 Protocolos

El recurso Top 5 de los Protocolos proporciona una vista de los protocolos de tráfico de la internases mas vistas. En la tabla siguiente al cuadro se proporciona el tipo de protocolo, la cantidad de datos, el número total de paquetes, y el porcentaje de todo el tráfico sobre la interfaz de ver con cada protocolo en la lista.

Top 5 Aplicaciones

El recurso Top 5 de aplicaciones proporciona una vista rápida de las aplicaciones más utilizadas por la interfaz de vista. En la tabla siguiente al cuadro se proporciona el nombre de la aplicación, la cantidad de datos que está fluyendo, el número total equivalente de los paquetes, y el porcentaje de todo el tráfico que es detectable con el uso de la aplicación de la lista de la interfaz de vista. Al hacer clic se abre una aplicación de la vista NetFlow aplicación. Para obtener más información, consulte "NetFlow Application View" en la página 37.

Top 5 Conversaciones

Este recurso proporciona una lista de las conversaciones de la creación de la mayor parte del tráfico sobre la interfaz de vista. Para cada conversación, este recurso informa de la cantidad de datos transferidos en la conversación y el porcentaje de la conversación lista representa del total de datos transferidos a través de la interfaz de vista. Al hacer clic en una conversación se abre la vista de NetFlow de conversación para la conversación seleccionada. Para obtener más información, consulte la sección "NetFlow Conversations View (vistas de conversaciones NetFlow)" en la página 41.

Top 5 Endpoints (Puntos finales o extremos)

El Top 5 de los recursos extremos ofrece una visión de los extremos de producción de la mayor parte del tráfico en la interfaz seleccionada. En la tabla siguiente al cuadro se proporciona el nombre o la dirección IP de cada extremo de la lista, la cantidad de tráfico de cada extremo de la lista, tanto en bytes y paquetes, y el porcentaje de todo el tráfico sobre la interfaz de vista que es atribuible a cada extremo de la lista. Al hacer clic en un extremo abre la vista NetFlow de punto final para el punto final seleccionado. Para obtener más información, consulte "NetFlow Endpoint View (vista de punto final de NetFlow)" en la página 41.

Top 5 Domains (Top 5 Dominios)

Este recurso proporciona una visión de los dominios que producen la mayor parte del tráfico en la interfaz seleccionada. En la tabla siguiente al cuadro se proporciona el nombre del dominio, la cantidad de tráfico en bytes, el número total de paquetes comunicado, y el porcentaje de todo el tráfico en la interfaz seleccionada que es atribuible a cada dominio.

Nota: Este recurso sólo está disponible si la resolución de DNS persistente está habilitada. De forma predeterminada en las instalaciones de evaluación, resolución de DNS está configurado para aparecer en la demanda solamente. Para obtener más información, consulte "Configuración de DNS y NetBIOS Resolución" en el *SolarWinds Orion NetFlow Traffic Analyzer Guía del administrador.*

Node Interfaces (Nodo de interfaces)

Este recurso proporciona una lista de todas las interfaces de control en el nodo visto. Para cada interfaz, tanto el tráfico entrante y saliente se informará. Al hacer click sobre una interfaz se abrirá una vista detallada de interfaces de NetFlow para ver los detalles de la interfaz seleccionada. Para obtener más información, consulte "Ver detalles de la interfaz de NetFlow" en la página 44.

Capítulo 4

Uso de Orion NetFlow Traffic Analyzer

Mientras Orion Network Performance Monitor puede decir el uso de ancho de banda en una interfaz, Orion NTA aprovecha esta capacidad un paso más allá, al proporcionar información sobre el usuario actual de ese ancho de banda y las aplicaciones que están utilizando. Los escenarios presentados en este capítulo ilustran el valor de Orión NTA y la forma en que inmediatamente le puede ofrecer un importante retorno de su inversión.

Adición de hablador superior a alertas de estadísticas de Orion

El software de alerta de Orión puede alertar sobre la encuesta, syslog, y los datos de trampa. Las alertas se definen en términos de condiciones relativas a los datos en la base de datos de Orión. Analiza en forma de consultas SQL a intervalos establecidos en los cuales se registraron valores que superen un determinado umbral, lo que provocó una alerta si pertenecen a condiciones pertinentes.

Cuando una alerta de Orión está activada, el software evalúa los criterios de supresión. Si el aviso no está calificado para ser suprimido, el programa ejecuta una acción definida. Si no se define, el software sólo muestra la alerta en la web de la consola.

A lo largo de este flujo de trabajo se utilizan temporizadores para permitir que el software haga su labor en cada paso y para garantizar que en el flujo de trabajo de alerta había redundancia adecuada para la presentación oportuna de las alertas.

Para un excelente panorama de alerta en Orión avanzada de alertas, consulte: Understanding Orion Advanced Alerts (comprendiendo alertas Orion). Para obtener toda la información específica sobre las alertas de Orión básicas y avanzadas, incluyendo las instrucciones detalladas para crear y administrar con el Administrador de Orión alerta, consulte el Capítulo 11, "Creación y administración de alertas," en la Guía del Orion Performance Manager Administrador.

Alertas Avanzadas del hablador superior

Al instalar SolarWinds Orion Network Traffic Analyzer, el software crea automáticamente en el Orion Alert Manager dos alertas predefinidas llamadas "High Reciba por ciento de utilización de traductores de Arriba" y "Alto porcentaje de utilización de transmisión con traductores de Arriba".

El propósito principal de estas alertas es ayudar en la comprensión de que tráfico de red en particular contribuyo más en alcanzar el umbral de ancho de banda con la interfaz, lo que provocó la alerta de rango de utilización.

De forma predeterminada, estas alertas avanzadas, cuando se activan, hacen dos cosas: 1) escribe el caso de utilización de ancho de banda en el registro de sucesos SolarWinds cuando el porcentaje de utilización actual en la transmisión del lado de una interfaz se eleva por encima del valor especificado, y luego otra vez cuando la utilización cae por debajo de un valor especificado. 2) Iniciar una red de captura de la información más actual del hablador superior y luego añadir y enviar esa información en un correo electrónico a los destinatarios configurados.

En las instrucciones de esta sección se presupone que está familiarizado con el Administrador de Orion de alerta y ya sabes cómo configurar una alerta avanzada.

Para conocer los pasos en la creación de una alerta avanzada consulte las secciones sobre las alertas avanzadas en el capítulo 11, "Creación y Gestión de Alertas," en la Guía del Orion Performance Manager Administrador.

Para utilizar la alerta NetFlow por defecto "de alto por ciento de utilización de transmisión con traductores de Arriba":

1. Abra el Orion Alert Manager (gerente de alertas Orion) en el grupo de programas de Orion.
2. Navegue hacia la gestion de alertas de recursos (**View** > **Configure Alerts**).
3. Seleccion la alerta de hablador superior correspondiente.
4. Click **Edit**.
   a. En **General**, check **Enable** (hablilitar) esta Alerta y selecciona una frecuencia de alerta evaluative.
   b. En condiciones de disparo, definir las condiciones en las que el software lanza la alerta.

      La condición predeterminada es la interfaz de transmitir utilización porcentaje superior a 75. Puede ajustar esta condición o añadir condiciones.
   c. En condiciones de reinicio, definir las condiciones en que el software reinicia la alerta.

      La condición predeterminada es la interfaz de porcentaje transmitida por debajo de 50. Puede ajustar esta condición o añadir condiciones.

d. Sobre eliminación de alerta, definir las condiciones en que el software suprime la alerta.

La condición predeterminada es sin supresión.

e. En la hora del día, definir los días y horas durante el cual el software activamente evalúa la base de datos para condiciones de disparo.

El rango por defecto es 24 / 7.

f. En desencadenar acciones, crear acciones a ejecutar cuando el software desencadena la alerta.
Como se mencionó, la acción predeterminada escribe en el registro de sucesos de SolarWinds, inicia una captura web de los actuales hablantes superiores de transmisión de la interfaz sobreexplotadas, y luego añade y envia la información por correo electrónico a un contacto apropiado.

Nota: En la ficha **URL**, si ha cambiado la entrada de Orión por defecto de 'Admin' con una contraseña en blanco, en consecuencia tendrá que cambiar la dirección **URL** que la acción de disparo para enviar la notificación.

Por ejemplo, si sus credenciales nuevas nombre de usuario “**NTA de usuario**” con la contraseña “**Bravo**”, usted modificará la dirección por defecto de forma que:

```
${SQL:SELECT REPLACE(REPLACE(Macro, '$$Password$$',
''),'$$User$$', 'Admin') FROM NetFlowAlertMacros WHERE
ID='InWebMailInterfaceDetailsLink'}
```

Se convierta en:

```
${SQL:SELECT REPLACE(REPLACE(Macro, '$$Password$$',
'Bravo'),'$$User$$', 'NTA User') FROM NetFlowAlertMacros
WHERE ID='InWebMailInterfaceDetailsLink'}
```

g. En condición de reinicio, definir las acciones a ejecutar cuando el software restablece la alerta. .

Como se mencionó, la acción predeterminada restablecida se escribe en el registro de sucesos de SolarWinds.

5. Click **OK** y luego click **Done**. (Hecho)

Para utilizar la opción predeterminada NetFlow "Alta Capacidad de utilización por ciento con habladores superiores de" alerta:

1. Abra el Administrador de alertas de Orión en el grupo de programas de Orión.

2. Vaya a la Gestión de los recursos Alertas de recursos (**Ver> Configuración de alertas**).

3. Seleccione la alerta correspondiente de transmisor superior.
4. Haga clic en **Edit**.
   a. En general, de verificación Habilitar esta Alerta y seleccione un alerta Evalutation frecuencia.
   b. El disparador Estado, definir las condiciones en que el software lanza la alerta.

      La condición predeterminada es la interfaz con utilización de transmición con porcentaje superior a 75. Puede ajustar esta condición o añadir condiciones.
   c. El condiciones de reinicio, definir las condiciones en que el software reinicia la alerta.

      La condición predeterminada es el porcentaje de la interfaz recibida utilizada por debajo de 50. Puede ajustar esta condición o añadir condiciones.
   d. Sobre la eliminación de alerta, definir las condiciones en que el software suprime la alerta.

      La condición predeterminada es sin represión.
   e. En la hora del día, definir los días y horas durante el cual el software activo evalúa la base de datos para condiciones de disparo.

      El rango por defecto es 24 / 7.
   f. En desencadenar acciones, crear acciones a ejecutar cuando el software desencadena la alerta.

      Como se mencionó, la acción predeterminada escribe en el registro de sucesos de SolarWinds, inicia una captura web de los hablantes superior actuales que reciben en la interfaz sobreexplotadas, y luego añade y envía la información por correo electrónico a un contacto apropiado.

      Nota: En la ficha URL, si ha cambiado la entrada de Orión por defecto de 'Admin' con una contraseña en blanco, en consecuencia tendrá que cambiar la dirección URL que la acción de disparo utiliza para enviar la notificación.

      Por ejemplo, si sus credenciales nuevas nombre de usuario “NTA de usuario” con la contraseña “Bravo”, usted modificará la dirección por defecto de forma que:

```
${SQL:SELECT REPLACE(REPLACE(Macro, '$$Password$$',
''),'$$User$$', 'Admin') FROM NetFlowAlertMacros WHERE
ID='InWebMailInterfaceDetailsLink'}
```

      Se convierta en:

```
${SQL:SELECT REPLACE(REPLACE(Macro, '$$Password$$',
'Bravo'),'$$User$$', 'NTA User') FROM NetFlowAlertMacros
WHERE ID='InWebMailInterfaceDetailsLink'}
```

g. En condición de reinicio, definir las acciones a ejecutar cuando el software restablece la alerta. .

Como se mencionó, la acción predeterminada restablecida se escribe en el registro de sucesos de SolarWinds.

5. Click **OK** y luego click **Done**. (Hecho)

Usando el Traffic View Builder

Usando el recurso el Builder (contructor) de vista de tráfico, usted puede generar sus propios puntos de vista personalizados para cualquier dispositivo de flujo activado. Traffic View Builder le permite crear sus propias versiones de cualquiera de los puntos de vista en la siguiente tabla.

Traffic View Builder Tipos de vistas		
Aplicación	País	Dominio
Endpoint (punto final)	Interface	Dirección grupo IP
Protocol (protocolo)	Router	Tipo de servicio

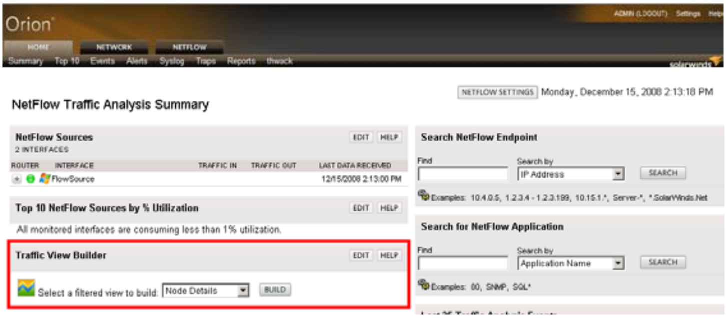
Las siguientes secciones presentan escenarios que muestran cómo el recurso Builder (constructor) de vistas de Orion NTA le permite crear sus propios puntos de vista.

Viendo el tráfico de una dirección IP designada

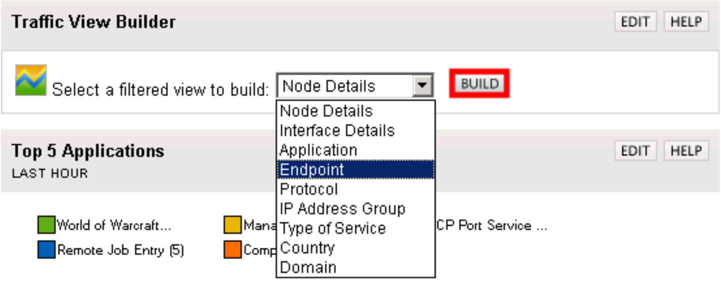
El siguiente procedimiento se crea una costumización de Orión vista NTA mostrando el tráfico de red entrante y saliente de una dirección IP designada.

To create a view for a specific IP address:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.



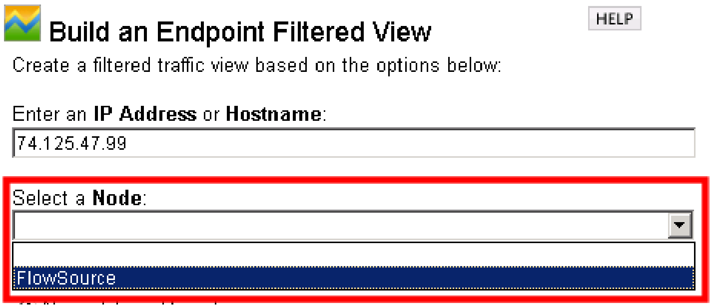
2. En el recurso Traffic View Builder, selecciona **Endpoint**, y luego haz click **Build**.



3. Entra la **IP address** (dirección IP) que usted desea monitorear.



4. Selecciona el **Node** (Nodo) que esta mandando tráfico a su dirección de IP seleccionada)



5. Selecciona **All Interfaces** (todas las interfaces) cuando en la sección se muestra un menú de la interfaz.

   Nota: Además, usted puede personalizar la vista para mostrar sólo el tráfico en una interfaz específica en el router, pero, a los efectos de esta evaluación, selecciona **All Interfaces** (todas las interfaces) para ver todo el trafico que atraviesa el router seleccionado.



6. Click **Submit**, y luego tu pantalla de tus puntos finales NetFlow customizados.

   Nota: Para obtener más información acerca de la opinión de NetFlow de punto final y de sus recursos predeterminados, consulte "Punto final NetFlow Ver" en la página 39.

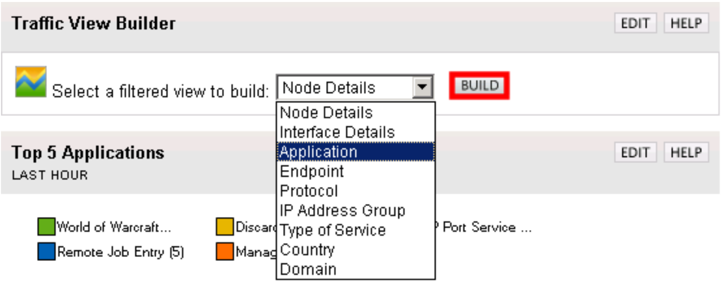
Viendo el tráfico de puertos específicos o aplicaciones

El siguiente procedimiento crea una vista customizada de Orión NTA que muestra el tráfico de red a través de puertos específicos o aplicaciones designadas.

Para crear una vista de puertos específicos y aplicaciones:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.

2. En el recurso de construcción de vista de tráficos, selecciona **Application**, y luego click **Build**.

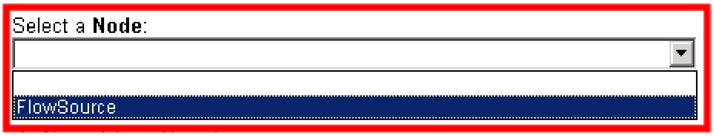


3. Selecciona la **Application** (aplicación) o el Puerto que deseas monitorear.

   Nota: Las solicitudes se presentan por número de puerto asociado. Para determinar la aplicación de las asociaciones de número de puerto, utilice el recurso de búsqueda de NetFlow de aplicaciones en el análisis de tráfico NetFlow vista Resumen. Para obtener más información, consulte el apartado "Búsqueda por Applicatio" en la página 31



4. Selecciona el Flow-enabled **Node** (Nodo flujo-habilitado) que esta enrutando su tráfico de información.



5. Selecciona **All Interfaces** (todas las interfaces) cuando la selección muestra un menú de la interfaz.

   Nota: Además, usted puede personalizar la vista para mostrar el tráfico de las aplicaciones sólo sobre una interfaz específica en el router, pero, a los efectos de esta evaluación, seleccione todas las interfaces para ver todo el tráfico a través del router seleccionado.



6. Click **Submit**, y luego su aplicación NetFlow customizada se mostrará.

Nota: Para obtener más información acerca de la opinión de NetFlow de aplicación y sus recursos predeterminados, consulte "NetFlow vista de aplicación" en la página 35.

Localización y aislamiento de un equipo infectado

Usted puede utilizar el actualmente instalado Orion NPM ejemplo, con la adición de Orión NTA, para identificar y responder rápidamente a la gran variedad de virus de propagación propia, que pueden atacar la red. Considere el siguiente escenario:

1. La sucursal local de su red de bancos que maneja todas las transacciones de tarjeta de crédito se queja de una red extremadamente lenta, causando interrupciones frecuentes durante la transferencia de datos sensibles.
2. La consola web Orion muestra que la conexión con la red de oficinas está por ensima.
3. Los gráficos Orion NPM de porcentaje de utilización en el programa de redes Resume que en páginas de inicio la utilización actual es del 98%, a pesar de que la utilización normal de la red de sucursales es 15-25%.
4. Usted haga click en **NetFlow Traffic Analysis** en la barra de herramientas del módulo, y luego haga click en el nombre del enlace red de sucursales en el recurso NetFlow Fuentes para ver el flujo habilitado del router en la red de sucursales.
5. Echando un vistazo rápido a los 5 puntos finales de los recursos, se ve que un solo equipo en la `10.10.10.0-10.10.10.255` intervalo de direcciones IP está generando el 80% de la carga en el vínculo filial.
6. Usted sabe que los ordenadores en este rango de direcciones IP son accesibles a los clientes para las transacciones personales utilizando la web.

7. Al ver el recurso Top 5 de aplicaciones, verá rápidamente que el 100% de las dos últimas horas de tráfico desde un ordenador de acceso público se ha generado por una aplicación de mensajería de IBM MQSeries.
8. Al hacer clic en el manual MQSeries de IBM de mensajería nombre de la aplicación en el Top 5 de los recursos de aplicaciones, que son capaces de determinar que IBM de mensajería MQSeries se produce a través del puerto 1883.
9. Sabiendo que no tiene ningún dispositivo utilizando MQSeries de IBM de mensajería en la ubicación del cliente de acceso, ni cualquier otro servicio o protocolos que requieren el puerto 1883, usted deberia reconocer que se trata de un virus “exploit”.
10. Usando una herramienta de gestión de configuración, como Network Configuration Manager Configuration Manager, pulse una nueva configuración de su firewall que bloquea el puerto 1883.

Localizando y bloqueando un uso involuntario

Con Orion NTA, usted puede fácilmente aumentar el uso gráfico en cualquiera de sus enlaces ascendentes de red diferentes. Orion NPM ya permite la utilización del cuadro, pero con la adición de Orión NTA, puede encontrar casos concretos de uso no deseado, lo que le permite tomar de inmediato medidas correctivas, como en el siguiente escenario:

1. Su subida a la Internet ha ido disminuyendo progresivamente en los últimos 6 meses, a pesar de que su recuento de las empresas, el uso de aplicaciones y ancho de banda dedicado han sido estables.
2. Cuando se abre la consola web de Orion, el Resumen de red muestra la vista que su principal vínculo de sitio de Internet, pero, al hacer clic en el enlace ascendente específica y consulta el porcentaje de utilización actual de cada interfaz gráfica, verá que la utilización actual de la interfaz de cara a la web es de 80%.
3. Haga clic en la interfaz de cara a la web para abrir la vista la interfaz de Datos.
4. Personalización de la tabla de porcentaje de utilización para mostrar los últimos 6 meses, se ve que ha habido un crecimiento constante del consumo del 15% al 80% en el tiempo. Incluso hay picos en los altos 90s.
5. Haga clic en la ficha Análisis de tráfico NetFlow, a continuación, haga clic en la web frente a la interfaz para abrir la interfaz de NetFlow vista Detalles.
6. En cuanto a los 50 **EndingPoints** (puntos finales), se ve que un grupo de equipos en el interfvalo de direcciones IP `10.10.12.0-10.10.12.255` está consumiendo la mayor parte del ancho de banda. Estos equipos residen en su rango de direcciones IP de las ventas internas.

7. Usted comienza a perforar en cada uno de los infractores las direcciones IP, y cada dirección IP a investigar muestra Kazaa (puerto 1214) y World of Warcraft (puerto 3724) de uso en el Top 5 aplicaciones.
8. Usando una herramienta de gestión de configuración, como Network Configuration Manager Configuration Manager, pulse una nueva configuración de su servidor de seguridad que bloquea los puertos 1214 y 3724.
9. En cuestión de minutos, verá el tráfico en la caída de la interfaz de nuevo a 25%.

Reconociendo la negación y frustración de los ataques de servicio (SYN Flood Attack)

Orion NTA le permite caracterizar fácilmente tanto el tráfico entrante y saliente. Esta capacidad es cada vez más importante como las redes corporativas están expuestas a la negación cada vez más dañina de los ataques de servicio. Considere el siguiente escenario:

1. Una alerta avanzada de Orion NPM le dirá que su router esta teniendo un problema creando y manteniendo estable la conexión a Internet.
2. Abra la consola Web de Orion para buscar posibles problemas. Todas las conexiones estan actualmente arriba y la utilización de ancho de banda se ve bien.Pero usted nota que el uso de se CPU en el nodo de firewall. Se está manteniendo constante entre el 99% y 100%.
3. Al hacer click en el nombre del servidor nodo de seguridad abrirá la página de Detalles del nodo donde el porcentaje de utilización actual de cada recurso interfaz y mostrará las interfaces del servidor de seguridad que están recibiendo niveles anormalmente altos de tráfico.
4. Haga clic en **NetFlow Traffic Análisis** (NetFlow análisis de tráfico) en la barra de herramientas de módulos para echar un vistazo rápido a su medida 50 de mejores recursos extremos.
5. El Top 50 de los recursos extremos muestra que los seis primeros ordenadores que intentan acceder a su red son extranjeros.
6. Te das cuenta de que los puertos están siendo escaneados y que el servidor de seguridad de forma interactiva está bloqueando estos ataques.
7. Usando una herramienta de gestión de configuración, como el gestor de configuración Network Configuration Manager, pulse una nueva configuración de su firewall que bloquea todo el tráfico en el rango de direcciones IP de los equipos que intentan acceder a su red.
8. En cuestión de minutos, la utilización de la CPU en su web, frente router vuelve a la normalidad.

Investigando Orion NTA más allá.

Aunque esto llega a la conclusión de la visita guiada de Orion NetFlow Traffic Analyzer, esta Guía de Evaluación no ha de ninguna manera cubierto totalmente la cantidad de caracteristicas de flujo activado de la red de monitoreo disponibles con Orion NTA. Por favor explore los SolarWinds Orion NetFlow Traffic Analyzer la guia del administrador, disponible en la página web SolarWinds, en http://www.solarwinds.com/support/documentation.aspx, para aprender aún más sobre el poder y la conveniencia de Orion NetFlow Traffic Analyzer.